Executive's Guide to IT Governance

Founded in 1807, John Wiley & Sons is the oldest independent publishing company in the United States. With offices in North America, Europe, Asia, and Australia, Wiley is globally committed to developing and marketing print and electronic products and services for our customers' professional and personal knowledge and understanding.

The Wiley Corporate F&A series provides information, tools, and insights to corporate professionals responsible for issues affecting the profitability of their company, from accounting and finance to internal controls and performance management.

Executive's Guide to IT Governance

Improving Systems Processes with Service Management, COBIT, and ITIL

ROBERT R. MOELLER

WILEY
John Wiley & Sons, Inc.

Cover image: © Max Delson Martins Santos/iStockphoto
Cover design: © John Wiley & Sons, Inc.

Copyright © 2013 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600, or on the Web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Moeller, Robert R.
Executive's guide to IT governance : improving systems processes with service management, COBIT, and ITIL / Robert R. Moeller.
1 online resource. — (Wiley corporate F&A series)
Includes bibliographical references and index.
Description based on print version record and CIP data provided by publisher; resource not viewed.
ISBN 978-1-118-22495-3 (pdf) — ISBN 978-1-118-23893-6 (epub) — ISBN 978-1-118-26354-9 (mobipocket) — ISBN 978-1-118-13861-8 (o-book) — ISBN 978-1-118-54017-6 (cloth)
1. Information technology—Management. 2. Information technology—Auditing.
3. Electronic data processing departments—Auditing. I. Title.
HD30.2
004.068'4—dc23

2012050404

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Dedicated to my best friend and wife, Lois Moeller.
Lois has been my companion and partner for over 40 years,
whether we are on our Lake Michigan sailboat,
skiing in Utah or elsewhere,
visiting museums and traveling to interesting places in the world,
vegetable gardening in the backyard,
or jointly cooking its produce.

Contents

Preface xiii

PART I: IT GOVERNANCE CONCEPTS

Chapter 1: Importance of IT Governance for All Enterprises 3

Chapter 2: Fundamental Governance Concepts and Sarbanes-Oxley Rules 9

Sarbanes-Oxley Act 10
Other SOx Rules—Title II: Auditor Independence 18
SOx Title III: Corporate Responsibility 22
Title IV: Enhanced Financial Disclosures 24
What Is IT Governance? 28
Notes 35

Chapter 3: Enterprise Governance and GRC Tools 37

The Road to Effective GRC Principles 38
Importance of GRC Governance 39
Risk Management Component of GRC 40
GRC and Enterprise Compliance 42
Importance of Effective GRC Practices and Principles 45

PART II: FRAMEWORKS TO SUPPORT EFFECTIVE IT GOVERNANCE

Chapter 4: IT Governance and COSO Internal Controls 49

Importance of Effective Internal Controls and COSO 50
COSO Internal Control Systems Monitoring Guidance 65

Wrapping It Up: Importance of COSO Internal Controls 66
Notes 66

Chapter 5: COBIT and the IT Governance Institute 67

An Executive's Introduction to COBIT 68
The COBIT Framework and Its Drivers 70
COBIT Principle 1: Establish an Integrated IT Architecture Framework 72
COBIT Principle 2: Stakeholder Value Drivers 74
COBIT Principle 3: Focus on Business Context 75
COBIT Principle 4: Governance and Risk Management Enablers 78
COBIT Principle 5: Governance and Management Performance Measurement Structures 80
Putting It Together: Matching COBIT Processes and IT Goals 81
Using COBIT in a SOx Environment 84
COBIT in Perspective 85
Notes 86

Chapter 6: ITIL and IT Service Management Guidance 87

ITIL Fundamentals 88
ITIL Service Strategy Components 91
ITIL Service Design 94
ITIL Service Transition Management Processes 99
ITIL Service Operation Processes 102
IT Governance and ITIL Service Delivery Best Practices 106
Note 107

Chapter 7: IT Governance Standards: ISO 9001, 27002, and 38500 109

ISO Standards Background 110
ISO 9000 Quality Management Standards 112
ISO IT Security Standards: ISO 27002 and 27001 115
ISO 38500 IT Governance Standard 118
Notes 123

Chapter 8: IT Governance Issues: Risk Management, COSO ERM, and OCEG Guidance 125

Risk Management Fundamentals 126
COSO ERM Definitions and Objectives: A Portfolio View of Risk 134
COSO ERM Framework 136
Other Dimensions of the COSO ERM Framework 152
The OCEG GRC "Red Book," Risk Management, and IT Governance 153
Notes 157

PART III: TOOLS AND TECHNOLOGIES TO MANAGE THE IT GOVERNANCE INFRASTRUCTURE

Chapter 9: Cloud Computing, Virtualization, and Portable, Mobility Computing 161

Understanding Cloud Computing 162
IT Systems and Storage Management Virtualization 168
Smartphone and Handheld IT Device Governance Issues 175
Note 176

Chapter 10: Governance, IT Security, and Continuity Management 177

Importance of an Effective IT Security Environment 177
Enterprise IT Security Principles: Generally Accepted Security Standards 178
Importance of an Effective, Enterprise-Wide Security Strategy 185
IT Continuity Planning 186
The Business Continuity Plan and IT Governance 188
Notes 193

Chapter 11: PCI DSS Standards and Other IT Governance Rules 195

PCI DSS Background and Standards 196
Gramm-Leach-Bliley Act IT Governance Rules 203
HIPAA: Health Care and Much More 208
Notes 216

Chapter 12: IT Service Catalogs: Realizing Greater Value from IT Operations 217

Importance of IT Service Catalogs 219
Role of a Service Catalog in the IT Service Provider Organization 221
An IT Service Catalog's Content and Features 223
IT Service Catalog Management 224

PART IV: BUILDING AND MONITORING EFFECTIVE IT GOVERNANCE SYSTEMS

Chapter 13: Importance of IT Service-Oriented Architecture for IT Governance Systems 231

SOA Applications and Service-Driven IT Applications 232
SOA Governance, Internal Control Issues, and Risks 235
Planning and Building an SOA Implementation Blueprint 236
SOA and IT Governance 242
Notes 245

Chapter 14: IT Configuration and IT Portfolio Management **247**

IT Configuration Management Concepts 248
ITIL Best Practices for IT Configuration Management 250
The Configuration Management Database: An Often Difficult Concept 254
Establishing an Enterprise CMDB 255
IT Portfolio Management 259

Chapter 15: Application Systems Implementations and IT Governance **263**

The Systems Development Life Cycle: A Basic Application Development Technique 264
IT Rapid Development Processes: Prototyping 266
Enterprise Resource Planning and IT Governance Processes 268

Chapter 16: IT Governance Issues: Project and Program Management **275**

The Project Management Process 275
PMBOK Standards 277
Another Project Management Standard: PRINCE2 280
IT Systems Portfolio and Program Management 280
The Program Management Office (PMO), a Strong Governance Resource 284
Project Management, the PMO, and IT Governance 286
Note 286

Chapter 17: Service Level Agreements, itSMF, Val IT, and Maximizing IT Investments **287**

ITIL Service Management Best Practices and the itSMF 288
Open Compliance and Ethics Group (OCEG) Standards 292
Val IT: Enhancing the Value of IT Investments 298
Notes 305

PART V: MONITORING AND MEASURING ENTERPRISE MANAGEMENT AND BOARD GOVERNANCE

Chapter 18: Enterprise Content Management **309**

ECM Characteristics and Key Components in the Enterprise Today 310
ECM Processes and IT Governance 310
Creating an Effective ECM Environment in the Enterprise 314

Chapter 19: Internal Audit's Governance Role 319

Internal Auditing History and Background 320
Internal Auditing and the IT Auditor 323
Internal Audit's IT Governance Activities and Responsibilities 323
Internal Audit IT Governance Standards 329
Internal Audit IT Governance Procedures 329
Note 334

PART VI: IT GOVERNANCE AND ENTERPRISE OBJECTIVES

Chapter 20: Creating and Sustaining an Ethical Workplace Culture 337

Importance of Mission Statements 337
Enterprise Codes of Conduct 340
Whistleblower and Hotline Functions 347
Launching an Ethics Program and Improving Enterprise Governance Practices 352
Note 353

Chapter 21: Impact of Social Media Computing 355

What Is Social Media Computing? 356
Social Media Examples 358
Enterprise Social Media Computing Risks and Vulnerabilities 365
Social Media Policies 367
Notes 370

Chapter 22: IT Governance and the Audit Committee's IT Role 371

The Enterprise Audit Committee and IT Governance 371
Audit Committee IT Governance Responsibilities 374
Audit Committee Briefings and IT Governance Issues 375

About the Author 377

Index 379

Preface

IN TODAY'S WORLD OF EVER-CHANGING ECONOMIC CONDITIONS and increased regulatory activities, governance is becoming an increasingly important issue for all sizes of enterprises, whether public corporations, not-for-profits, or private businesses. Enterprise governance concepts consist of a series of broad areas of enterprise activity, starting first with management's accountability and fiduciary responsibilities to its customers, employees, regulators, and all other stakeholders. This requires the implementation of guidelines and programs to ensure that management acts in good faith and that the overall enterprise is protected from wrongdoing or fraud. In addition, enterprise governance includes management processes and policies to promote strategic and economic efficiency. The management of economic efficiency involves how the corporate governance system intends to optimize results and meet its objectives. This promotion of strategic efficiency also calls for an enterprise to promote and establish public policy objectives that are not always directly measurable in economic terms but include such things as a strong ethics program, the promotion of quality, and employee welfare.

Effective enterprise governance, of course, requires strong management skills to make important decisions and provide leadership. There is also a very strong requirement for information technology (IT) systems and processes in particular. This important area, IT governance, is the overall topic of this executive guide.

In the earlier days of IT systems and processes, senior operations management often delegated many aspects of IT operations to specialists responsible for building, operating, and maintaining an enterprise's IT resources. While there was frequent talk about engaging the management and users of IT systems with the specialists and developers of their IT resources, operations management often experienced disappointments. New IT initiatives often did not meet their planned objectives, were delivered late, had security and internal control vulnerabilities, or too soon became obsolete due to poor planning or assessments of management needs. To improve matters today, there is a need for better processes to manage and coordinate all aspects of an enterprise's IT resources—the need for IT governance.

This book is an executive's guide to this important concept of IT governance. Our focus is not on the IT specialist installing IT hardware, software, and network connections, nor on such important resources as internal auditors who test and review IT processes. Rather, this guide is directed to the enterprise executive who has some understanding of IT processes but is interested in learning more about the issues and processes

that are important for efficiently managing and benefiting from these IT resources and systems in today's Internet-connected environment.

A goal of this book is to provide high-level background information on a variety of IT governance issues that are important to today's business enterprise and executive manager. We hope to provide that business executive with sufficient general information to allow him or her to have a greater understanding of important IT governance issues today and to be able to better ask questions that will achieve a greater understanding of these issues and better make effective decisions regarding these IT governance matters. For example, business literature today frequently makes reference to a concept called *cloud computing*. Chapter 9 will provide an overview of cloud computing and why it is important for effective IT governance. Similarly, we will introduce the concept of service level agreements (SLAs), often informal contracts between the users or owners of IT resources and IT management. Our objective here is to help the business executive better understand why SLAs are important, how to install and manage them in all sizes or types of enterprises, and how to use them to improve IT governance processes.

We have divided the chapters following into six basic topics or section areas. Each of these sections and their associated chapters is generally complete, summarizing IT governance issues in that area, and can hopefully serve the business executive with enough high-level information to understand each of these IT governance concepts and issues.

- **Part I—IT Governance Concepts.** The chapters in this section start by providing an overall introduction to the concept of IT governance and how it applies to business enterprises in general, and then to their IT resources. This section includes a chapter that describes the importance and impact of Sarbanes-Oxley Act (SOx) rules, an important set of legislation first initiated in the United States early in this century and now an almost-worldwide set of regulations mandating general rules for enterprise finance and other internal controls. This part concludes with a chapter explaining overall governance, risk, and compliance (GRC) issues, an important concept and term common in many enterprise-level management discussions today.
- **Part II—Frameworks to Support Effective IT Governance.** Beyond high-level IT governance concepts and standards, an enterprise executive needs to have an understanding of some of the high-level frameworks that are important for both IT and overall enterprise governance. A chapter here provides an overview of the Committee of Sponsoring Organizations (COSO) internal control framework and why it is important for effective IT governance. In addition, a chapter will provide an overview and introduction to the Control Objectives for Information and related Technology framework, known by the acronym COBIT, as well as supporting guidance from the IT Governance Institute. Both of these are important internal control concepts, and an enterprise business executive should have an understanding of both as well as why they are important for IT governance.

  A chapter in this part will also introduce another very important IT governance concept, known as the Information Technology Infrastructure Library (ITIL), a set of best practices guidance materials for managing all aspects of an enterprise's IT resources. Related to ITIL, the chapter also will introduce the IT

Service Management Forum, an important professional organization that provides IT governance guidance. A business executive, with responsibilities for managing IT operations, should have at least a good understanding of these guidance materials, their use in an IT function, and how they promote more effective IT governance.

Chapters in the first part of this book also introduce two other frameworks important to IT governance. First, we will discuss several ISO, or International Organization for Standardization, sets of guidance materials important for IT governance. We also introduce the OCEG, or Open Compliance and Ethics Group, set of risk management guidance. An understanding of both ISO IT governance standards and OCEG is important for implementing effective IT governance practices. These frameworks should help an enterprise manager understand some important IT governance issues.

- **Part III—Tools and Technologies to Manage the Governance Infrastructure.** The IT infrastructure includes all of the people and resources needed to run and manage the IT facility for an enterprise, including the IT server hardware, IT security specialists, and both the people and hardware to manage the IT telecommunications network. A chapter in this section discusses several important newer technologies that are changing IT today, such as the concepts of cloud computing and what is known as *virtualization*. We will introduce these and other related issues and discuss why they are important for IT governance.

  IT infrastructures face a variety of security and integrity threats, such as the risk of an unexpected attack from rogue software, the failure to restore operations because of a lack of backed-up key systems, or password violations that result in improper access to confidential data. One chapter here will introduce IT security and continuity planning issues that are important for effective IT governance. Another chapter will introduce some of the more important IT security rules and regulations that are important for establishing effective IT governance.

  We will then conclude this part with a chapter on techniques for realizing greater value from IT operations. IT governance should consist of both well-controlled and well-managed operations and efficient and cost-effective IT processes. Management at all levels should have a general understanding of how to implement and benefit from these issues, and this chapter will offer some guidance from an IT management perspective.
- **Part IV—Building and Monitoring Effective IT Governance Systems.** In addition to IT infrastructure processes and tools from the previous section, the chapters here discuss approaches for building effective IT governance processes in the systems and applications found in enterprises. In particular, one of these chapters introduces and discusses the importance in what is generally called *service-oriented architecture,* an increasingly common approach to building and implementing new applications but a set of processes rather different from the conventional techniques of earlier IT development approaches. Other chapters in this part will discuss IT governance issues for managing systems and process changes and revision controls as well as approaches to implement integrated systems for the better governance and management of IT operations.

There is a chapter in this section on tools and techniques for project and program management. Management at all levels should understand the importance and value of good project management and control techniques to promote IT governance processes. This part then concludes with a chapter on service level agreements—formal performance standards and measures between an IT resource and its user community, and a very important IT governance tool.

- **Part V—Monitoring and Measuring Enterprise Management and Board Governance.** Many of the earlier chapters focus on helping the IT executive to understand and implement effective IT governance processes in an enterprise's IT systems and operations. This section introduces the role of the internal audit, and a chapter discusses the importance of internal audit for IT governance.

  Another chapter here discusses document management approaches from an IT executive perspective, including the importance of data content management and data archiving issues.
- **Section VI—IT Governance and Enterprise Objectives.** This final section concludes with some guidance on creating and sustaining an ethical workplace culture, an important element in IT governance. We also have a chapter here on the importance of social network computing—the growing use of such tools as Facebook and their overall impact on IT governance. The last chapter concludes the book with guidance on using IT governance to communicate the business value of IT.

These chapters are focused on the needs and interests of the senior enterprise business executive. In each of the chapters following, we will begin by explaining why the chapter topic is important from an IT governance perspective. We will then discuss tools and techniques to implement the particular governance processes as well as approaches for measuring their success. In addition to the specific chapters on these topics, many other chapters will draw on important elements from IT service management, COBIT, and ITIL processes. We will try to link all specific IT governance issues with general enterprise governance controls and concerns.

An overall objective of this book is to help senior enterprise managers to better understand important IT governance issues today and to help implement them in their enterprise. The result should be stronger systems and processes both for IT and for the overall enterprise.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

PART ONE

IT Governance Concepts

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER ONE

Importance of IT Governance for All Enterprises

COMPUTERS AND INFORMATION TECHNOLOGY (IT) applications first burst into the business world primarily in the United States and Europe starting in the early 1960s. It was a new business technology then and many companies were offering competing computer hardware and software products to major corporations at that time. Companies at all levels wanted to get up to speed with this new technology, and massive investments were made in installing new systems and hiring and training the programmers and analysts to build and launch them. Despite some failures along the way, we are all using and benefiting today from these types of computer hardware and software products.

Today, IT systems supported by ever-changing and improving technologies are a major component of almost all business activities. However, our IT activities have not been supported by some of the same standards and procedures found in other business areas. For example, accounting systems and financial standards are supported by recognized accounting principles that are reviewed by independent auditors and follow governmental financial accounting rules, such as those of the Securities and Exchange Commission in the United States. Similar best practices rules and standards exist for other areas of business activity, such as in many aspects of marketing and quality control. This is not the case for IT systems and processes. Despite the fact that IT operations are facing increasing governmental and professional compliance requirements and face a wide range of systems-related risks, there is an ongoing need for better IT governance practices today.

IT governance is a concept that was almost unknown not too many years ago. We thought about enterprise governance from the roles and activities of senior management and the board of directors, but IT functions in those earlier enterprises were just viewed as very important support functions and not as major business activities. Our overall thinking of enterprise governance really changed in the United States in the early years

of this century after the failure of a major U.S. corporation called Enron. That failure was so sudden and almost unexpected that U.S. governmental regulators investigated and found that many corporate governance and financial practices were lacking. The result was the Sarbanes-Oxley Act (SOx) in the United States. These legislative rules have had a major impact on financial reporting and corporate governance practices, first in the United States and then worldwide. Sarbanes-Oxley has also had a major related impact on the need for effective IT governance.

Today, senior managers, IT managers, and practitioners think of IT governance in many varying but different ways. Some see IT governance as "command-and-control" rules over IT initiatives imposed by internal auditors, non-IT executives, and outside consultants; others consider it a corporate mechanism that implements a Big Brother approach to apply top-down constraints to overall IT activities. From the perspective of the IT practitioner who is building and managing systems to improve business productivity, IT governance is sometimes seen as an unnecessary evil that hampers IT-related creativity and productivity in the enterprise. In any case, IT governance does not impose upon enterprise management and their IT functions with stringent regulations, standards, and policies. Rather, good IT governance is a set of policies and best practices that should serve as a strategic enabling force to improve enterprise business operations. It is embraced by all levels in the organization and reaches far beyond the four walls of IT enterprise operations.

Good IT governance aligns an enterprise strategically to support the evolution of an IT architecture that delivers consistent and scalable business value. IT governance helps measure a business's growth and success, including its financial health. The chapters following present an emerging and comprehensive view of IT governance that addresses enterprise root business performance criteria along with the important factors of compliance adherence and risk management. As the chapters following discuss important aspects of each, we will refer to governance, risk, and compliance factors by their initials, *GRC*. This is an acronym that is frequently found in business publications today.

IT governance is about the way an enterprise accomplishes the delivery of mission-critical business capabilities using IT strategies, goals, and objectives. IT governance is concerned with the strategic alignment between the goals and objectives of the business and the utilization of its IT resources to effectively achieve the desired results. Exhibit 1.1 shows this IT governance concept and how it fits in with overall enterprise strategies.

Although Exhibit 1.1 is very general, it shows IT governance concepts—the purpose of this book—in the center but within overall enterprise strategies and operations. This is always a key concept to keep in mind. Too often, an aggressive IT director may tend to think that his or her ideas for improving and running IT systems and operations are almost more important than other enterprise activities. We should always keep in mind that although IT operations are usually critical to overall business operations, they must fit into overall business activities and strategies. Although the head of IT, the enterprise chief information officer (CIO), may feel that he or she has the best idea for some change or improvement in IT operations, that idea should be subservient to other corporate activities. For example, a CIO may recognize the importance of implementing service level agreements (SLAs), or informal contracts between users and IT, as discussed in Chapter 17, and as a good way to improve IT operations.

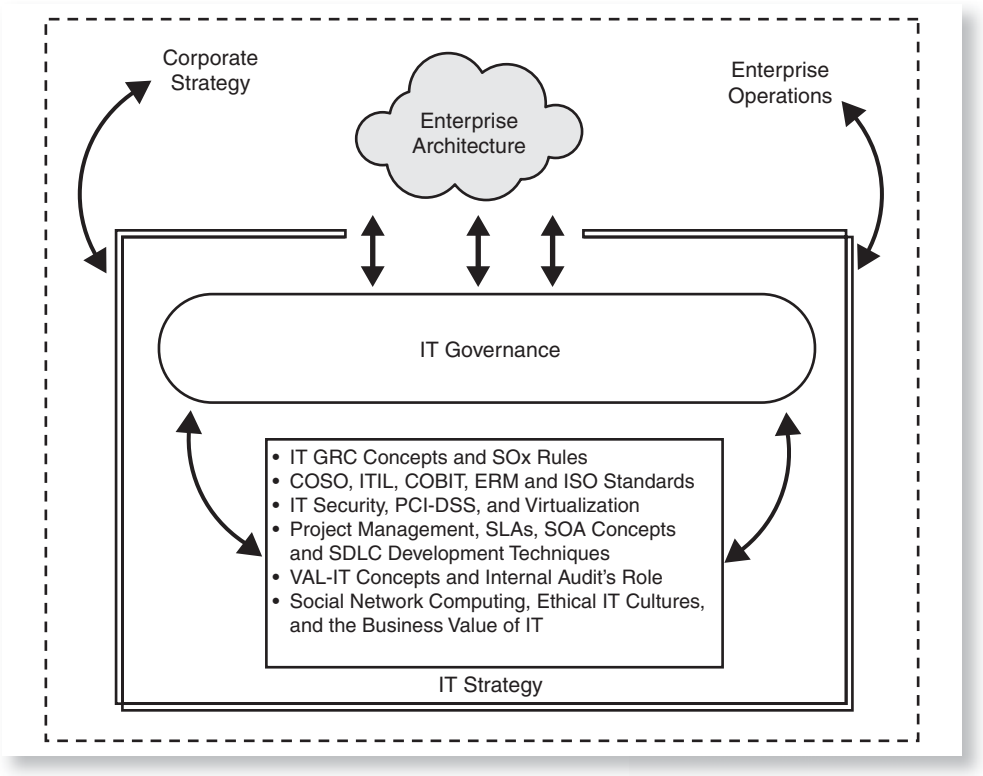
Corporate Strategy
Enterprise Architecture
Enterprise Operations
IT Governance
• IT GRC Concepts and SOx Rules
• COSO, ITIL, COBIT, ERM and ISO Standards
• IT Security, PCI-DSS, and Virtualization
• Project Management, SLAs, SOA Concepts and SDLC Development Techniques
• VAL-IT Concepts and Internal Audit's Role
• Social Network Computing, Ethical IT Cultures, and the Business Value of IT
IT Strategy

EXHIBIT 1.1 IT Governance Concepts

If senior management does not like this idea, the CIO should accept senior management's direction and go forward and make other improvements where possible.

Our point here is that enterprise IT architecture sets the overall big-picture rules for enterprise activities and IT governance. The chapters following suggest many areas for improving IT systems and operations. With an objective of improving overall enterprise IT governance, however, all of these IT governance improvements must fit into the big picture of corporate operations.

The IT governance section in Exhibit 1.1 points to a series of other activities. Each of these roughly corresponds to the chapter topics outlined in the Preface to this book and described in the chapters going forward. In them, we have tried to outline many of the issues that are important for improving IT governance. They must be closely connected with links to overall business operations.

IT governance disseminates authority to the various layers in the organizational structures within the business, while ensuring appropriate and prudent use of that authority. This does not refer simply to hierarchical structures; we should always remember that network structures allow for specialization, teaming, and building infrastructure to support those teams. Specialization allows the sum of the parts of the organization to be greater than the whole. We should also remember that IT governance is not only for large organizations. Smaller enterprises have a need for good IT governance

practices as well. However, there are obviously a smaller number of control points to be deployed in a smaller operation, and the focus of our chapters points to the larger enterprise.

As the chapters following have defined it, IT governance affects business performance, and it ideally helps an enterprise to outperform its competition. A key theme here is that IT governance *defines* business performance, specifically the performance of IT resources as they are applied to the business's strategic objectives. Good IT governance leads directly to increased productivity, higher quality, and improved financial results. Poor IT governance, on the other hand, often leads to programmatic waste, bureaucracy, lower morale, and diminished overall financial performance.

To underscore the importance of good IT governance practices, consider the production of goods or services for typical enterprise business customers. These customers generally have visibility into a business only where they interface for the purpose of ordering or making requests, receiving value through the sale or production of products, or providing information through surveys or marketing analyses. It is the efficiency and coordination of internal business processes that comprise end-to-end customer experience; this is an aspect of business performance and should be measured and improved. In order to positively impact business performance, IT governance process must have focus and visibility on these overall end-to-end business processes with which customers interact. Poor IT governance loses sight of the customer in favor of satisfying regulations, standards, and policies *in isolation.* Local gains in process efficiency and productivity often do not provide favorable results in the context of the end-to-end business processes. Furthermore, the implementation of externally imposed regulations on internal business processes must be accounted for in ways that positively impact customer experiences, not simply as the apparent overhead of compliance; doing otherwise simply introduces risk into an enterprise. Good IT governance addresses whole end-to-end business processes and coordinates the activities of the enterprise over time and across organizational boundaries.

IT governance, as discussed in these chapters, should not be considered just in a new enterprise initiative. It is not a project that separately begins and ends but rather should be a key element in the fabric of an enterprise that transcends time, leadership, and other initiatives. Whether enterprise IT governance processes have grown unintentionally through evolving process improvements or grown intentionally through a deliberate project, the questions a senior manager should ask include: "How good are my IT governance processes at effectively delivering strategic business value year after year?" and "Are my processes repeatable, predictable, and scalable, and are they truly meeting the needs of my business (outside of IT) and my customers?"

It is no more likely that a single IT governance process will work for all IT business processes than it is for every one of an enterprise's customers to be satisfied with the exact same product or service configuration for any given product or service that a company produces. Therefore, a number of IT governance-related processes must be considered. This integrated collection of available IT governance processes is what we describe in the chapters following as the *IT governance landscape.*

IT governance is a subset of enterprise governance, which at the highest level drives and sets what needs to be accomplished by improving overall management processes.

IT governance itself encompasses systems, the overall IT infrastructure, and communications. Product development governance, like IT governance, is a subset of enterprise governance and overlaps with IT governance. Product development governance is targeted for enterprises that develop products (as opposed to IT service delivery discussed in Chapter 17, for example). IT development governance should be applied to development organizations and programs, and is a subset of IT and product development governance.

The chapters following introduce and describe many important frameworks and concepts—with names such as COBIT or ITIL—that are well understood by many IT professionals but may be less familiar to the senior enterprise executive. However, these are all important tools and processes to improve enterprise IT governance, as Chapter 2 will discuss. In our IT-centric world today, the senior enterprise executive should understand why IT governance and the related concepts of IT-related compliance activities and risk management are important. This is an overall goal of this book.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER TWO

Fundamental Governance Concepts and Sarbanes-Oxley Rules

AS WE DISCUSSED IN CHAPTER 1, the term *enterprise IT governance* is not new, but is a concept that has meant different things to different people. The concept of enterprise governance has been evolving over recent years, at least in the United States. As a response to ongoing cycles of business frauds and failures particularly in the latter decades of the past century, there has been an increased emphasis on embellishing enterprise codes of conduct and establishing what are called corporate ethics departments. This author got involved in corporate governance issues when he directed the internal audit function for a large U.S. corporation and was asked to chair a task force and take leadership for the company to revise many internal rules, rewrite its code of conduct, and establish an ethics function for that company in response to a major threat of litigation involving consumer fraud. Strong enterprise governance practices were established for that company, although they emphasized general operations and with little emphasis on IT systems and operations.

Enterprise governance issues became increasingly important in the first years of this century when the United States experienced a series of major corporate failures that were generally caused by accounting misdeeds and financial fraud. The notorious poster boy for this period was the commodities trading firm Enron. Its sudden and unexpected failure was based on financial fraud and caused several corporate executives to go to prison. Enron's failure precipitated passage of the Sarbanes-Oxley Act (SOx) in the United States, as well as similar requirements worldwide. The sections following will provide an overview of SOx's internal controls and governance legislation.

The general governance concepts that were discussed in Chapter 1 take a somewhat different direction when we introduce information technology (IT) concepts and systems into the mix. Many of our general management governance concepts were established and somewhat perfected during the last half of the twentieth century. Standards were established, as were work practices between management and external auditors and regulators.

In addition to our overview of SOx concepts, this chapter provides a high-level review of IT governance issues, including their IT-related enterprise risk, security, and legislative issues. The chapter will discuss some of the internal and external threats that impact enterprise IT governance processes as well as some of the characteristics of effective IT governance in the enterprise. This chapter surveys both general and specific IT governance concepts as they apply to today's senior manager. Many of these concepts also will be referenced and discussed in greater detail in other specific topic chapters.

SARBANES-OXLEY ACT

The Sarbanes-Oxley Act is a U.S. law enacted in 2002 to improve public company financial reporting, audit, and enterprise governance processes. It first had a major impact on businesses in the United States and now is recognized worldwide. Although SOx's auditing and internal control rules have directly changed many external auditor and IT financial practices, SOx has also had a major impact on IT governance. A general understanding of SOx, with an emphasis on its Section 404 internal accounting control rules, is a key knowledge requirement for all senior managers.

SOx became a U.S. law as a response to a series of accounting misdeeds and financial failures at such once-major corporations as Enron and WorldCom. SOx has caused major changes that have impacted corporate governance, accounting, and financial reporting audit processes—first in the United States and now worldwide. Although SOx is a comprehensive set of legislation with many components, most of its business and auditor attention has focused on the SOx Section 404 internal control attestation rules. These internal control audit procedures have caused a major amount of effort and concern as corporations began to establish compliance with SOx. This section provides a high-level overview of SOx today, with an emphasis on its Section 404 and the rules that are most important for IT governance issues. We will summarize SOx requirements for reviews of internal accounting controls and will summarize the relatively new external auditing standard called Auditing Standard No. 5 (AS5), a set of more risk-based auditing approaches that also emphasizes the importance of performing financial reporting internal control reviews. All senior enterprise managers should have a general knowledge and understanding of SOx internal control rules.[1]

Sarbanes-Oxley Act Key IT Governance Elements

The official name of SOx is the Public Accounting Reform and Investor Protection Act. It became law in August 2002, with most of the final detailed rules and regulations released by the end of the following year. Its title being a bit long, business professionals refer to it as the Sarbanes-Oxley Act from the names of its principal congressional sponsors. Most generally refer to it today as SOx, SOX, or Sarbox, among many other variations.

SOx introduced a series of totally changed processes for external auditing and gave new governance responsibilities to senior executives and board members. SOx also established the Public Company Accounting Oversight Board (PCAOB), a rule-setting

authority under the Securities and Exchange Commission (SEC) that issues financial auditing standards and monitors external auditor governance. As happens with all financial and securities-related federal laws, an extensive set of specific regulations and administrative rules has been developed by the SEC based on the SOx legislation.

U.S. federal laws are organized and issued as separate sections of legislation called Titles, with numbered sections and subsections under each. Much of the SOx legislation contains rules that are not that significant for many business professionals. For example, Section 602(d) of Title I states that the SEC "shall establish" minimum professional conduct standards or rules for SEC practicing attorneys. While perhaps good to know, this does not have any enterprise management or IT governance impact. Exhibit 2.1 summarizes the major titles or sections of SOx, although our focus will only be on SOx's Titles I and IV. Our intent is not to describe all sections of SOx or to reproduce the full text of this legislation—it can be found on the Web[2]—but to highlight portions of the law that are more significant to interested business professionals. We will start with a discussion of SOx's Title I, the PCAOB, and the Section 404 rules.

EXHIBIT 2.1 Sarbanes-Oxley Act Key Provisions Summary

Section	Subject	Rule or Requirement
101	Establishment of PCAOB	Overall rules for the establishment of the PCAOB, including its membership requirements.
104	Accounting Firm Inspections	Schedule for PCAOB inspections of registered public accounting firms.
108	Auditing Standards	The PCAOB will accept current but will issue its own new auditing standards.
201	Out of Scope Practices	Outlines prohibited accounting firm practices such as internal audit outsourcing, bookkeeping, and financial systems design.
203	Audit Partner Rotations	The audit partner and the reviewing partner must rotate off an assignment every 5 years.
301	Audit Committee Independence	All audit committee members must be independent directors.
302	Corp. Responsibility for Financial Reports	The CEO and CFO must personally certify their periodic financial reports.
305	Officer and Director Bars	If compensation is received as part of fraudulent or illegal accounting, the benefiting officer or director is required to personally reimburse funds received.
404	Internal Control Reports	Management is responsible for an annual assessment of internal controls.
407	Financial Expert	One audit committee director must be a designated financial expert.
408	Enhanced Review of Financial Disclosures	The SEC may schedule extended reviews of reported information based on certain specified factors.
409	Real-Time Disclosure	Financial reports must be distributed in a rapid and current manner.
1105	Officer or Director Prohibitions	The SEC may prohibit an officer or director from serving in another public company if guilty of a violation.

SOx Title I: Public Company Accounting Oversight Board

SOx introduced significant new rules for external auditors. Prior to SOx, the American Institute of Certified Public Accountants (AICPA) had guidance-setting responsibility for all external auditors and their public accounting firms through its overall responsibility for the Certified Public Accountant (CPA) certification. While state boards of accountancy actually licensed CPAs, the AICPA previously had overall responsibility for the profession. External audit standards also were set by the AICPA's Auditing Standards Board (ASB). Although basic standards—called generally accepted auditing standards (GAAS)—have been in place over the years, newer auditing standards were released as numbered Statements on Auditing Standards (SASs). Much of GAAS was just good auditing practices, such as that accounting transactions must be backed by appropriate documentation, while the SASs covered specific areas requiring better definition. SAS No. 99, for example, covered the consideration of fraud in a financial statement audit. The AICPA's code of professional conduct required CPAs to follow and comply with all applicable auditing standards.

The AICPA's GAAS and its numbered SAS standards had been accepted by the SEC, and these auditing rules defined external auditing standards and the tests necessary for an audited financial statement. However, the accounting scandals that led to the passage of SOx signaled that the AICPA-led process of establishing auditing standards was "broken." SOx took this audit standards-setting process away from the AICPA, which was dominated by the major public accounting firms, and created the PCAOB, a nonfederal, nonprofit corporation with the responsibility to oversee all audits of corporations subject to the SEC.

The PCAOB does not replace the AICPA but assumes responsibility for the external auditing practices for AICPA members. The AICPA continues to administer the CPA examination, with its certificates awarded on a state-by-state basis, and sets auditing standards for U.S. private, non-SEC organizations. While SOx Title I defines PCAOB auditing practices for external auditors, other audit process and corporate governance rules have changed how internal auditors coordinate their work with external auditors. Although SOx Title I contains many new rules, perhaps the three most important to many senior managers are that the PCAOB now has major responsibility for public accounting firms, now sets their external auditing standards, and sets audit standards rules such as workpaper retention. The following paragraphs briefly describe these SOx Title I external audit process rules:

PCAOB administration and public accounting firm registration. The PCAOB is administered through an SEC-appointed board with required membership that is not dominated by CPA and public accounting firm interests. The PCAOB is responsible for overseeing and regulating all public accounting firms that practice before the SEC and for establishing auditing standards.

Auditing, quality control, and independence standards. The PCAOB has the authority to establish auditing and related attestation standards and quality control and ethics standards for registered public accounting firms. SOx recognizes previously issued AICPA auditing standards and has issued a limited number of new standards to

date, such as AS5 for the review and evaluation of internal controls. SOx rules further specify that an external auditor's evaluation must contain a description of material weaknesses as well as any material noncompliance matters found. External auditors are required to update the effectiveness of internal controls, and an absence of this documentation should be considered a weakness of internal controls.

Audit workpapers retention. Workpapers are the documentation prepared by auditors during an audit. PCAOB standard AS3, Audit Documentation, mandates that audit workpapers and other supporting materials should be maintained for a period of not less than seven years. This requirement is certainly in response to an infamous event just prior to the fall of Enron and its then auditor, Arthur Andersen. Enron was still in operation but was under some financial pressures when the SEC announced that it was going to conduct an onsite investigation. Enron's then external auditor, Arthur Andersen, used an internal firm policy to justify destruction of all but the most current of their Enron audit documentation. This was a motivating factor that led to this SOx rule.

Scope of internal control testing. PCAOB rules require external auditors to describe the scope of both their testing processes and test findings. Prior to SOx, external auditors had sometimes used internal firm policies to justify the most minimal of test sizes, and they frequently tested only a very small number of items despite being faced with very large test populations. If no problems were found, they expressed an opinion for the entire population based on the results of a very limited sample. They now must pay greater attention to the scope and reasonableness of their testing procedures, and the supporting documentation must clearly describe the scope and extent of testing activities.

Title IV: Enhanced Financial Disclosures and Section 404

SOx Title IV is designed to correct some financial reporting disclosure problems, to tighten up conflict-of-interest rules for corporate officers and directors, to mandate a management assessment of internal controls, to require senior officer codes of conduct, and other matters. There is a lot of material here, but the most significant nugget for most senior managers is Section 404 on Management's Assessment of Internal Controls. SOx requires that all annual 10K reports must contain an internal controls report stating management's responsibility for establishing and maintaining an adequate system of internal controls as well as management's assessment, as of the fiscal year ending date, on the effectiveness of those installed internal control procedures. This is what has popularly been known as the Section 404 rules. Internal and IT auditors, outside consultants, or even the management team—but not the external auditors—have the responsibility to review and assess the effectiveness of their internal controls, and external auditors are then to attest to the sufficiency of these internal control reviews built and controlled by management.

Section 404 reviews are supported by the AS5 standards discussed later in this section and are particularly important to internal auditors because the rules specify that external auditors may elect to use the work of internal auditors in their internal control reviews.

SOx Section 404 rules state that an enterprise is responsible for reviewing, documenting, and testing its own internal accounting controls, with those review results then passed on to the enterprise's external auditors, who are charged with reviewing and attesting to that work as part of their review of the reported financial statements. When SOx first became law, Section 404 reviews were a major point of concern for many enterprises because external auditors were following a very detailed set of financial accounting audit procedures defined in the earlier PCAOB Auditing Standard No. 2 (AS2) that required a very detailed review approach that did not give any allowances for small errors or omissions. Section 404 auditing rules subsequently have changed with the release of AS5 in 2007, a more risk-based audit approach that also allows external auditors to better use the work of internal auditors in their assessments.

Section 404 Internal Controls Assessments

Management always has had the overall responsibility for designing and implementing internal controls over their enterprise's operations. Although the standards for what constituted good internal controls were not always very well defined in the past, they have remained a fundamental management concept. SOx Section 404 requires an annual internal controls report, with the following information elements, as part of an SEC-mandated Form 10K annual report:

- A formal management statement acknowledging the enterprise's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
- An assessment, as of the end of the most recent fiscal year, of the effectiveness of the enterprise's internal control structure and procedures for financial reporting.

In addition, the external audit firm that issued the supporting audit report is required to review and report on management's assessment of its internal financial controls. Simply put, management is required to report on the quality of their internal controls, and their public accounting firm must audit or attest that management developed an internal controls report in addition to their normal financial statement audit. Management has always been responsible for preparing their periodic financial reports, and the external auditors then audited those financial numbers and certified that they were fairly stated. With SOx Section 404, management is responsible for documenting and testing their internal financial controls as well as to report on their effectiveness. External auditors then review the supporting materials leading up to that internal financial controls report to assert that the report is an accurate description of the internal control environment.

To the non–financial statement auditor and certainly to many senior business executives, this might appear to be an obscure or almost trivial requirement. Even some internal auditors who primarily perform operational audits may wonder about the nuances in this process. However, audit reports on the status of internal controls have been an ongoing issue between external auditors, the SEC, and other interested parties going back to at least 1974. Much of the problem then was that there was no recognized definition for what is meant by internal controls.

The COSO internal control framework discussed in Chapter 4 describes an accepted standard for understanding internal controls. Under SOx Section 404, management is required to report on the adequacy of their internal controls, with their external auditors attesting to the management-developed internal control reports.

This process follows a basic internal control such as the importance of maintaining a separation of duties where the person who develops transactions should not be the same person who approves them. Under Section 404 procedures, the enterprise builds and documents its own internal control processes, then an independent party such as internal audit reviews and tests those internal controls, and finally the external auditors review and attest to the adequacy of this process. Their financial audit procedures will be based on these internal controls. This Section 404 process improves things from pre-SOx days when external auditors frequently built, documented, and then audited their own internal controls—a separation-of-duties shortcoming.

Identifying Key Processes to Launch a Section 404 Compliance Review

Whether based on IT systems or primarily manual procedures performed on a regular basis, every enterprise has basic processes that are normally considered in terms of their basic accounting cycles, including:

- **Revenue cycle.** Processes dealing with sales or other enterprise revenue.
- **Direct expenditures cycle.** Expenditures for material or direct production costs.
- **Indirect expenditures cycle.** Operating costs that cannot be directly tied to production activities but are necessary for overall business operations.
- **Payroll cycle.** Covers all personnel compensation.
- **Inventory cycle.** Although inventory will eventually be applied as direct production expenditures, time-based processes are needed for holding inventory until applied to production.
- **Fixed assets cycle.** Property and equipment require separate accounting processes, such as periodic depreciation accounting over time.
- **General controls IT cycle.** This set of processes covers IT controls that are general or applicable to all IT operations.

The identification of these key enterprise processes is an initial Section 404 compliance step, and an enterprise should document, understand, and test all of these "key processes." For many enterprises, these are prime systems and supporting IT processes that have been reviewed through annual external audit reviews.

Internal Audit's Role

Even though SOx does not give specific responsibilities to internal audits, they are an important resource for the completion of Section 404 internal control assessments. Under SOx, a separate and independent function within the enterprise—often internal or IT audit—reviews and documents the internal controls covering key processes, identifies key control points, and then tests those identified controls. External audit would then review that work and attest to their adequacy. For many enterprises, IT audit can be a key resource for performing these internal controls reviews for technology-based processes.

Senior financial management and the audit committee should work with the enterprise's external auditors to define responsibilities for their Section 404 internal control reviews. They are performed on an annual process, with documentation prepared and tested in the first year, then updated and retested in future periods. All parties should develop a cost-effective approach to achieve these SOx requirements and assess their IT applications and controls.

SOx Section 404 reviews should be planned and conducted similarly to many new IT projects, as discussed in Chapter 19 on internal audit's IT governance role. Exhibit 2.2 outlines some planning considerations for a Section 404 internal control review to be performed by an enterprise's internal auditors, who can play a major role in helping senior

EXHIBIT 2.2 Planning Considerations for a Section 404 Internal Control Review

1. Determine status of review—Is this the first round of Section 404 reviews for the entity and a subsequent-year follow-up?
2. If a new review, follow the work steps to understand, document, and test key processes. Otherwise, plan for a subsequent-period review.
3. Review the detailed documentation covering prior 404 reviews, including process flow charts, internal control gaps identified and remediated, as well as overall project planning documentation for prior review.
4. Review any recently published PCAOB rules covering Section 404 reviews and related auditing changes, and adjust review procedures to reflect those changes.
5. Meet with the external audit firm responsible for the current Section 404 attestations and determine if there are any changes in documentation and testing philosophy, with an emphasis on AS5 rules, from that prior review.
6. Consider any organization changes since the past review, including acquisitions or major reorganizations, and modify review coverage, if necessary.
7. Through meetings with senior and IT management, identify if new systems or processes have been installed over the past period and if those new changes have been reflected in updated documentation.
8. Review any internal control weaknesses identified in the past review and assess whether internal control corrections reported as installed appear to be working.
9. Assess the status of existing Section 404 documentation and determine the extent of new documentation preparation necessary.
10. Assuming the prior Section 404 review was done by internal audit, determine that appropriate knowledgeable trained resources are available to perform the upcoming review.
11. Interview all parties involved in the prior Section 404 review exercise to assess any lessons learned and develop plans for corrective actions in the upcoming review.
12. Based on discussions with external auditors and senior management, determine scope materiality parameters for the upcoming review.
13. Determine that the software, if any, used to document prior review is still current, and make any changes necessary to have adequate tools in place to perform the upcoming review.
14. Prepare a detailed project plan for the upcoming Section 404 review, with considerations given to coordination of review activities at business entity units and external auditors.
15. Submit plan for approval by senior management.

management establish Section 404 compliance. Our objective is not to provide internal audit guidance but to give a senior manager an idea of these IT internal audit processes.

AS5 Rules and Internal Audit

Shortly after SOx became law in the United States, the PCAOB released its AS2 guidance that called for external auditors to take very conservative and detailed approaches on their audits of financial statements. AS2 mandated a "look-at-everything" detailed audit approach, and enterprise external audit bills became much more expensive in those first SOx years. However, there were frequent complaints by industry leaders and others, with a general consensus that AS2 needed some revisions. The SEC and the PCAOB agreed to revise AS2, and AS5 was issued in late May 2007.

AS5 is a set of standards for the external auditors who review and certify published financial statements, and these rules are also important for internal auditors as well. AS5 introduces risk-based rules with an emphasis on the effectiveness of internal controls that are more oriented to enterprise facts and circumstances. In addition, AS5 calls for external auditors to consider including reviews of appropriate internal audit reports in their financial statement audit reviews. It allows external auditors to place more emphasis on management's ability to establish and document key internal controls.

AS5 rules are particularly important for internal auditors because external auditors can rely on the work of internal auditors in their Section 404 assessments. AS5 has three broad objectives:

1. **Focus internal control audits on the most important matters.** AS5 calls on external auditors to focus their reviews on areas that present the greatest risk that an internal control will fail to prevent or detect a material misstatement in financial statements. This approach calls for external auditors to focus on identifying material weaknesses in internal control in their audits, before they result in material misstatements of financial statements. AS5 also emphasizes the importance of auditing higher-risk areas, such as the financial statement period-end close process and controls designed to prevent fraud by management. At the same time, this standard provides external auditors a range of alternatives for addressing lower-risk areas, such as by more clearly demonstrating how to calibrate the nature, timing, and extent of testing based on risk, as well as how to incorporate knowledge accumulated in previous years' audits into the auditors' assessment of risk. Also and very important to internal auditors, AS5 allows external auditors to use the work performed by an enterprise's internal auditors when appropriate.
2. **Eliminate audit procedures that are unnecessary to achieve their intended benefits.** AS5 does not include the previous AS2 standard's detailed requirements to evaluate management's own evaluation process and clarifies that an internal control audit does not require an opinion on the adequacy of management's processes. For example, AS5 focuses on the multilocation dimensions of risk in an enterprise and reduces requirements that external auditors should test a "large portion" of an enterprise's operations or financial positions. This should allow a reduction in financial audit work.

3. **Make the financial audit clearly scalable to fit the size and the complexity of any enterprise.** In order to provide guidance for audits of smaller, less complex companies, AS5 calls for tailoring internal control audits to fit the size and complexity of the enterprise being audited. The standard has guidance on how to apply AS5 to smaller, less complex enterprises as well as the units of larger enterprises.

Following AS5, external auditors may consider using the work of others to help perform their SOx financial statement internal control audits. While this was not very well defined under previous SOx AS2 rules, AS5 now explicitly allows it. AS5 states that an external auditor may use the work performed by, or receive direct assistance from, internal auditors, other company personnel, or third parties working under the direction of management or the audit committee, to provide evidence about the effectiveness of financial reporting internal controls. This was a major change for internal auditors.

Of course, the external auditors are signing off on or attesting to the audit results, and they must assess the competence and objectivity of the persons whose work they plan to use. The higher the degree of competence and objectivity of others, the greater use an auditor may make of their work. In particular, AS5 calls for an assessment of the competence and objectivity of the internal auditors at an enterprise. Competence means the attainment and maintenance of a level of understanding and knowledge that enables persons to perform the tasks assigned to them, and objectivity means the ability to perform those tasks impartially and with intellectual honesty. To assess competence, an external auditor should evaluate the qualifications and ability of the internal auditors or others to perform the work the external auditor plans to use. To assess objectivity, AS5 calls for an external auditor evaluation of whether factors are present that either inhibit or promote a person's ability to perform with the necessary degree of objectivity the work the auditor plans to use.

AS5 goes on to state that external auditors should not use the work of persons who have "a low degree of objectivity, regardless of their level of competence," and also should not use the work of persons who have a low level of competence regardless of their degree of objectivity. Personnel whose core function is to serve as a testing or compliance authority at an enterprise, such as internal and IT auditors, normally are expected to have greater competence and objectivity in performing the type of work that will be useful to the external auditor. This is an area where the audit committee and senior management may want to challenge their external auditors if they see no role for internal audit in this financial statement audit planning process.

OTHER SOx RULES—TITLE II: AUDITOR INDEPENDENCE

Internal and external auditors have historically been separate and independent resources. External auditors were responsible for assessing the fairness of an enterprise's internal control systems and the resultant published financial reports, while internal auditors served management in a wide variety of other areas. In the early 1990s, this separation began to change, with external audit firms taking overall responsibility for some internal audit functions as well. This started when

larger enterprises began to "outsource" some of their noncore functions such as the employee cafeteria or a plant janitorial function. The thinking was that employees who worked in these specialized areas were not really part of core enterprise operations, and an enterprise's janitorial function or other noncore functions might be "outsourced" to another company that specialized in areas such as janitorial services for many other enterprises. The previous in-house janitors would then be transferred to the janitorial services company and, in theory, everyone would benefit. The enterprise that initiated the outsourcing would experience lower costs by giving a noncore function, janitorial services, to someone who better understood it. The outsourced janitor, in this example, also might have both better career possibilities and better supervision.

Internal audit outsourcing first got started in the late 1980s. External audit firms went to their client firm's management and offered to "outsource" or take over existing internal audit functions. The idea appeared to make sense to senior management and audit committees on many levels. Senior management often did not really understand the distinctions between the two external and internal audit functions and were sometimes more comfortable with their external auditors. In addition, senior management and audit committee members were often enticed by the promised lower costs of internal audit outsourcing, and internal audit outsourcing continued to grow through the 1990s. Although a few independent firms made efforts to get into this market, internal auditor outsourcing continued to be the realm of the major public accounting firms.

Internal audit outsourcing became very much of an issue in the Enron scandal, its internal auditor function having been almost totally outsourced to its external audit firm, Arthur Andersen. The two audit groups, both officially Andersen employees with different reporting relationships, worked side by side in Enron's offices. After Enron's fall, many raised after-the-fact questions about how that outsourced internal audit department could have been independent of Andersen. It would have been very difficult in this environment for internal audit to raise concerns to the audit committee about their external auditors. This potential conflict became a reform issue for SOx.

Limitations on External Auditor Services

SOx has made it illegal for a registered public accounting firm to contemporaneously perform both audit and non-audit services at a client. The prohibitions include internal auditing, many areas of consulting, and senior officer financial planning. The most significant element here is that it is illegal for a registered public accounting firm to provide internal audit outsourcing services if it is also doing the audit work. This means that the major public accounting firms are now essentially out of the internal audit outsourcing business for their direct audit clients. Other firms, including independent spin-offs from public accounting firms or specialized internal audit consulting firms, can still provide internal audit outsourcing, but the era when an internal audit professional became a contractor or employee of his or her public accounting firm is over.

In addition to the ban on providing outsourced internal audit services, SOx prohibits public accounting firms from providing other services, including:

- **Financial information systems design and implementations.** Public accounting firms had been installing financial systems—often of their own design—at clients for many years. They were then coming back and reviewing the internal controls of the systems they had just installed—a significant conflict of interest. This is no longer allowed.
- **Bookkeeping and financial statement services.** Public accounting firms previously offered accounting services to their clients in addition to doing the audits. Even for major corporations, it was not unusual for the team responsible for the overall financial statement audit to also do much of the work necessary in building the final consolidated financial statements. Again a potential conflict of interest, this is not allowed.
- **Management and human resources functions.** Prior to SOx, external audit firms often identified professionals from their own firms and helped move them to client management positions. The result was an environment where virtually all of the accounting managers in an enterprise often were alumni of their external auditors. This was sometimes frustrating for internal auditors or others who were not from that same public accounting firm. Avenues for promotion above certain levels seemed limited because of "old-boy" network connections with the external audit firm.
- **Other prohibited services.** SOx specifically prohibits external audit firms from offering actuarial services, investment advisory services, and audit-related legal services, although tax services are allowed.

The overall SOx theme here is that external auditors are authorized to audit the financial statements of their client enterprises, and that is about all. SOx allows that beyond the prohibited activities listed, external auditors can engage in other non-audit services only if those services are approved in advance by the audit committee. With the increased scrutiny of audit committees under SOx, many are typically wary of approving anything that appears to be at all out of the ordinary.

Audit Committee Preapproval of Services

Section 202 of SOx's Title I specifies that the audit committee must approve all audit and non-audit services *in advance.* While audit committees have or should have been doing this all along, that approval was often little more than a formality prior to SOx. Audit committees in the "old days" often received little more than a brief written and/or verbal report from a responsible audit department that was approved in the same perfunctory manner that business meeting minutes are often approved. SOx changed all of this, and audit committee members can now expose themselves to criminal liabilities or stockholder litigation for allowing a prohibited action to take place.

Of course, there are many minor matters regarding external auditor activities that should not have to go through this formal audit committee advance approval process.

Using legal terminology, SOx sets de minimus[3] exception rules for these audit committee permission requirements. Per SOx, preapproval is not required for some non-audit services if:

- The aggregate dollar value of the service does not exceed 5 percent of the total external audit fees paid by the enterprise during the fiscal year when the services were provided.
- The services were not recognized as non-audit service by the enterprise at the time the overall audit engagement was initiated.
- These services are brought to the attention of the audit committee and approved by it prior to the completion of the audit.

These exceptions give the external auditors and the audit committee some flexibility. However, the nature and accumulated dollar value of these additional non-audit services must be carefully monitored throughout the course of a fiscal year to maintain a level of compliance. Internal audit should become involved in this process to help ascertain that all provided extra services continue in compliance with the SOx rules, including disclosure to investors through the annual proxy statement. SOx does allow that the audit committee may delegate this non-audit services preapproval authority to one or more of the outside directors on the audit committee. This would relieve the strain of lengthy audit committee business matters, but put even more responsibility on a few audit committee members over and above the many new legal responsibilities mandated by SOx.

External Audit Partner Rotation

Another section of Title II makes it unlawful for a public accounting firm lead partner to head a specific engagement for over five years. This is a matter that the major public accounting firms had corrected well before SOx. Lead partners from the major firms had been rotated on a regular basis, although there may have been exceptions with smaller firms and smaller engagements. While lead partner rotation had been common, SOx makes the failure of a firm to rotate a criminal act. However, SOx does not really address the common practice in audit partner rotation where a given person will play the lead on an audit and then continue to serve in an advisory role after his or her term. That advisory role partner can often maintain the same level of responsibility as the designated lead partner and could become a potential violation of SOx rules.

As this book goes to press, there are rumors or comments that the PCAOB is considering requiring full public accounting firm rotation. At present, partners may rotate but the firm remains unchanged. The thinking is that a new firm will provide enterprise management with a new perspective on the audit process.

External auditors have always communicated regularly with their audit committees in the course of the audit engagement, as well as for any other matters of concern. In the aftermath of Enron and the other corporate scandals at that time, it was discovered that this communication was sometimes very limited. A member of management might negotiate a "pass" from the public accounting partner on a suggested accounting

treatment change, but the matter was only reported to the audit committee in the most general of terms, if at all.

SOx has changed this. External auditors are required to report on a timely basis all accounting policies and practices used, alternative treatments of financial information discussed with management, the possible alternative treatments, and the approach preferred by the external auditor. The whole idea here is that external auditors must report to their audit committee any alternative accounting treatments, the approach preferred by the external auditors, and management's approach. This really says that if there are disputed accounting treatments, the audit committee should be made well aware of the actions taken. This requirement really points to the need for good audit committee documentation.

Conflicts of Interest and Mandatory Rotations of External Audit Firms

It had once been common for members of the external audit firm team to get job appointments for senior financial positions at their audit clients. SOx Title II, Section 206, prohibits external auditors from providing any audit services to a firm where the chief executive officer (CEO), chief financial officer (CFO), or chief accounting officer participated as a member of that external audit firm on the same audit within the last year. This really says that an audit partner cannot leave an audit engagement to begin working as a senior executive of the same firm that was just audited. While staff members and managers can still move from the public accounting firm team to various positions in the auditee enterprise, this prohibition is limited to public accounting partners. There were some outrageous examples of this switching of roles as part of all of the news about Enron.

SOx TITLE III: CORPORATE RESPONSIBILITY

SOx's Title III regulations contain major regulatory rules for audit committees and prescribe audit committee performance standards and a large set of corporate governance rules. Under SOx, *all* registered enterprises must have an audit committee composed of only independent directors. The firm's external audit firm is to report directly to the audit committee, which is responsible for their compensation, oversight of the audit work, and the resolution of any disagreements between external audit and management. While major U.S. corporations have had audit committees, these rules were tightened from the past traditional practices. For example, while internal audit departments have had an often weak reporting relationship to their audit committees in past years, SOx has made this reporting link much stronger and more active.

Each member of the board's audit committee must be a totally independent director, and at least one member of the audit committee must be a "financial expert." These rules were introduced because in the hearings that led up to the enactment of SOx, it was discovered that some of Enron's audit committee members did not appear to understand many of the financial transactions they were being asked to review and approve.

SEC regulations define a "financial expert" as a person who, through education and experience, has:

- An understanding of generally accepted accounting principles and financial statements;
- Experience applying such generally accepted accounting principles in connection with the accounting for estimates, accruals, and reserves that are generally comparable to the estimates, accruals, and reserves, if any, used in the registrant's financial statements;
- Experience preparing or auditing financial statements that present accounting issues that are generally comparable to those raised by the registrant's financial statements;
- Experience with internal controls and procedures for financial reporting; and
- An understanding of audit committee functions.

These rules do not require any stiff certifications, academic backgrounds, or other qualification. They just say that members of an audit committee must present themselves as having some level of knowledge on accounting, financial reporting, and internal control issues. In some respects, an audit committee member is being asked to put herself or himself in the potential line of fire if the enterprise is ever questioned regarding some financial or internal control decision.

The SOx legislation also calls for audit committees to establish procedures to receive, retain, and treat complaints and handle whistleblower information regarding questionable accounting and auditing matters. This really says that an audit committee must become, in effect, an almost separate ongoing entity rather than a subset of the traditional board that flies to some location and meets quarterly. While this is a nice-sounding idea, most audit committee functions do not have the supporting resources to handle an enterprise-level whistleblower function—something that is often the responsibility of an enterprise's corporate-level ethics function. Despite the words in the SOx legislations, audit committee–level whistleblower functions today are run on essentially an ad hoc basis.

Prior to SOx, U.S. enterprises filed their financial statements with the SEC and published the results for investors, but the responsible corporate officers who "signed" or authored those reports were not personally responsible. The bar has now been raised. The CEO, the principal financial officer, or other persons performing similar functions must certify each annual and quarterly report filed. The signing officer, as part of what is referred to as Section 302, must certify that:

- The signing officer has reviewed the report.
- Based on that signing officer's knowledge, the financial statements do not contain any materially untrue or misleading information.
- Again based on the signing officer's knowledge, the financial statements fairly represent the financial conditions and results of operations of the enterprise.
- The signing officer is responsible for:
  - Establishing and maintaining internal controls.

  - Having designed these internal controls to ensure that material information about the enterprise and its subsidiaries was made known to the signing officer during the period when the reports were prepared.
  - Having evaluated the enterprise's internal controls within 90 days prior to the release of the report.
  - Having presented in these financial reports the signing officer's evaluation of the effectiveness of these internal controls as of that report date.
- The signing officer should disclose to the external auditors, audit committee, and other directors that any significant deficiencies in the design and operation of internal controls that could affect the reliability of the reported financial data have been disclosed to the enterprise's auditors.
- The signing officer should also indicate whether there were internal controls or other changes that could significantly impact those controls, including corrective actions, subsequent to the date of the internal control evaluation.

Given that SOx imposes potential criminal penalties of fines or jail time on individual violators of the act, the signer enterprise governance requirement places a heavy burden on responsible corporate officers. Corporate officers must take all reasonable steps to make certain that they are in compliance.

This personal sign-off requirement has raised major concerns from corporation CEOs and CFOs and causes a major amount of additional work for the accounting and finance staffs preparing these reports as well as signing officers. The enterprise needs to set up detailed paper-trail procedures such that the signing officers are comfortable that effective processes have been used and the calculations to build the reports are all well documented. An enterprise may want to consider using an extended sign-off process where staff members submitting the financial reports sign off on what they are submitting. Exhibit 2.3 is an example of an officer disclosure sign-off type of statement that officers will be requested to sign. While this exhibit is not an official PCAOB form, it is based on SEC documents, showing the types of things an officer will be asked to certify. We have highlighted a couple of phrases in Exhibit 2.3 in ***bold italics***. Under SOx, the CEO or CFO is asked to personally attest to these types of representations and could be held criminally liable if incorrect. While the officer is at risk, the support staff—including internal audit—should take every step possible to make certain that the package presented to the senior officer is correct.

TITLE IV: ENHANCED FINANCIAL DISCLOSURES

This title of SOx is designed to correct some financial reporting disclosure problems, to tighten up conflict-of-interest rules for corporate officers and directors, to mandate a management assessment of internal controls, to require senior officer codes of conduct, and other matters. There is a lot of material here. Many unexpected bankruptcies and sudden earnings failures about the time of the Enron failure around 2002 were attributed to extremely aggressive, if not questionable, financial reporting. With the approval

EXHIBIT 2.3 SOx Officer Disclosure Sign-off

CERTIFICATE OF EMPLOYEE REGARDING SARBANES-OXLEY COMPLIANCE

Certification: Understanding that we intend to rely upon these statements, the undersigned hereby certifies, represents, and warrants to each of them and to the Company as follows:

1. I have read those portions of the accompanying draft of the covered filing that relate directly to the scope of my responsibilities as an employee of the Company (the "certified information").

2. Based on my knowledge, the certified information, as of the end of the period covered by such filing, did ***not contain an untrue statement of a material fact*** or omit to state a material fact necessary to make the statements therein, in light of the circumstances under which they were made, not misleading.

3. Based on my knowledge, to the extent of the scope of the certified information, the certified information fairly presents, in all material respects, the financial condition, results of operations, and cash flows of the Company as of the close of and for the period presented in the covered filing.

4. I am not aware of any deficiencies in the effectiveness of the Company's disclosure controls and procedures that could adversely affect the Company's ability to record, process, summarize, and report information required to be disclosed in the covered filing.

5. I ***am not aware of any significant deficiencies or material weaknesses*** in the design or operation of the Company's internal controls that could adversely affect the Company's ability to record, process, summarize, and report financial data.

6. I ***am not aware of any fraud, whether or not material***, that involves the Company's management or other employees who have a significant role in the Company's internal controls.

Signature: _____.

Dated this _____ day of _____, 20xx.

Print Name:

Title:

of their external auditors, companies pushed to the limits and often used such tactics as issuing questionable pro forma earnings to report their results or moved the corporate headquarters offshore to minimize taxes. While these tactics were previously allowed at that time through generally accepted accounting principles (GAAP), international financial reporting standards (IFRS), and some existing laws, SOx changed many rules here and made these financial disclosure tactics difficult to use or illegal.

In a common tactic at that time, what were called pro forma financial reports were frequently used to present an "as-if" picture of a firm's financial status by leaving out nonrecurring earnings expenses such as restructuring charges or merger-related costs. However, because there is no standard definition and no consistent format for reporting pro forma earnings, depending on the assumptions used, it was possible for an operating loss to become a profit under pro forma earnings reporting.

The problem with two sets of numbers is that investors and the press frequently ignore the GAAP numbers, focusing on the more favorable pro forma results. SOx-mandated rules require that pro forma published financial statements must not contain any materially untrue statements or omit any fact that makes the reports misleading. Further, the pro forma results also must reconcile to the financial conditions and results of operations under GAAP.

Perhaps the major issue that brought Enron down was a large number of off-balance-sheet transactions that, if consolidated with regular financial reports, would have shown major financial problems. Once they were identified and included with Enron's other financial results, their disclosure pushed Enron toward bankruptcy. SOx now requires that quarterly and annual financial reports must disclose all such off-balance-sheet transactions that may have a material effect on the current or future financial reports. These transactions may include contingent obligations, financial relationships with unconsolidated entities, or other items that could have material effects on operations. The final rules here, after passage of Sox, require an enterprise to provide an explanation of its off-balance-sheet arrangements in a separately captioned subsection of the "Management's Discussion and Analysis" (MD&A) section of the annual Form 10K.

Expanded Conflict-of-Interest Provisions, Disclosures, and Codes of Ethics

The hearings that led to the passage of SOx often pictured corporate officers and directors as a rather greedy lot. In arrangements that frequently appeared to be conflicts of interest, large relocation allowances or corporate executive personal loans were granted and subsequently forgiven by corporate boards. A CEO, for example, who requests the board to grant his CFO a large personal "loan" with vague repayment terms and the right to either demand payment or forgive certainly creates a conflict-of-interest situation. Although a series of exceptions are allowed, SOx makes it unlawful for any corporation to directly or indirectly extend credit, in the form of a personal loan, to any officer or director.

As an important element of enterprise governance, SOx requires that corporations must adopt a code of ethics for their senior financial officers and disclose compliance with this code as part of their annual financial reporting. While SOx has made this a requirement for senior officers, employee codes of ethics or conduct have been in place in some enterprises for many years. They evolved to more formal ethics functions in larger corporations in the early 1990s, but were often established for employees and supervisors rather than for corporate officers. These codes defined a set of rules or policies that were designed to apply for all employees and covered such matters as policies on the protection of company records or on gifts and other benefit issues.

With a growing public concern about the need for strong ethical and governance practices, many enterprises have appointed an ethics officer to launch such an initiative, with a code of conduct as a first step. SOx does not address the content of these enterprise-wide codes of ethics, but focuses on the need for the same standards for senior officers as for all employees in the enterprise. SOx specifically

requires that an enterprise's code of ethics or conduct for its senior officers must reasonably promote:

- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;
- Full, fair, accurate, timely, and understandable disclosure in the enterprise financial reports; and
- Compliance with applicable governmental rules and regulations.

If an enterprise has a code of conduct, management should assure that this code applies to all members of the enterprise, is consistent with SOx, and that these ethical rules are communicated to all members of the enterprise, including the officers. The key governance issue here is making sure that the existing code of conduct covers the above SOx rules, that it has been communicated to senior management, and that these officers have agreed to comply with it. While SOx compliance processes must be established just for senior officers, this is the ideal time to launch an ethics function throughout the enterprise that applies to senior management and to all employees as well.

Not just a SOx legal requirement, a strong set of ethical standards can get an enterprise through a crisis situation and help it move in the right direction. A motivation for SOx and its strong provisions in these areas was the perception that certain corporate officers were operating on the basis of personal gain with no consideration for strong ethical values as evidenced by correct and accurate financial reporting. SOx's ethical requirements can help any enterprise to better set itself up for improved governance and ethical business conduct practices.

Other SOx Rules and Requirements

SOx also includes a large and complex set of rules covering such areas as audit committee governance requirements, security analyst conflicts of interest, and other financial disclosure rules. It is not our objective to provide a detailed summary of the overall legislation and its provisions. From the perspective of enterprise and IT governance, an understanding of Section 404 and some of the other issues highlighted in this chapter are perhaps the most significant. A more detailed general description of SOx can be found in this author's previously referenced book on SOx.

Passed as a U.S. law in the early 1990s, SOx is an important item of legislation that has since changed many aspects of financial reporting, internal control practices, and enterprise governance. Although some elements of SOx have changed since its original passage and its requirements did not really gather much additional compliance attention, most aspects of SOx are still active and applicable. The major area of change was the release of AS5, discussed previously, an auditing standard that prescribed a more risk-based approach to reviewing and assessing internal controls. SOx originally contained some whistleblower rules that allowed staff members to independently report potential financial fraud, with rewards for savings going to the person reporting. Though it was originally assumed that this would cause a storm of litigation, there has not been much if any SOx activity in this area since its passage.

Although many of its details will be handled by financial management as well as the external and internal auditors, today's business executive should have a good general understanding of SOx rules and requirements. The general description of SOx included in this chapter should help today's business executive to better understand SOx and its importance in IT governance.

WHAT IS IT GOVERNANCE?

As highlighted in the introduction to this chapter, the discipline of IT governance is a subset and very important element of overall enterprise governance issues. There is no single accepted definition of IT governance, and an Internet search shows that IT governance means different things to different people:

- IT governance is often used to describe the processes for deciding how money for IT resources should be spent. This IT governance process includes the prioritization and justification of IT investments. It includes controls on spending such as budgets and authorization levels.
- IT governance is often used to describe many different aspects of IT changes. At the low level, it is sometimes used to describe project management and control of a portfolio of IT-related projects, as described in Chapter 16.
- IT governance is used to make sure that IT change processes comply with regulatory requirements, both governmental laws and rules as well as professional standards.
- IT governance is the process of aligning IT change and expenditure to business requirements and expenditures. Sometimes it also covers the deployment of IT staff.
- IT governance is also used to describe the management and control of IT services. For example, service level agreements (SLAs), discussed in Chapter 17, are used to define levels of service that are acceptable to business, and then used as a basis for monitoring services.
- IT governance makes sure that day-to-day problem solving and support of all IT resources are aligned to business needs.

IT governance deals primarily with the connection between an enterprise's business focus and the IT-related management and operation of the enterprise. The concept highlights the importance of IT-related matters and emphasizes that strategic IT decisions should be owned by the most senior levels of corporate management, including the board of directors, rather than just IT management such as the chief information officer (CIO). IT governance concepts have really evolved since the earlier days of IT when senior management often handed over the authority and funding of IT operations to specialists with such titles as chief information officer (CIO) but did not aggressively manage IT resources from an overall management perspective.

The results of this process were some really outstanding IT processes that transformed many leading enterprises worldwide and improved their efficiency and profitability. However, over those same years many other enterprises experienced some

massive IT systems failures because of poor project planning, cost overruns, failures by the business and IT to understand IT issues, and other matters. For example, a 2002 Gartner survey found that 20 percent of all expenditures on IT are wasted—a finding that represents, on a global basis, an annual destruction of value totaling about $600 billion—and an IBM survey in 2004 of Fortune 1000 CIOs found that, on average, CIOs believe that 40 percent of all IT spending brought no return to their organization.[4] In recent years, other surveys have consistently revealed that 20 to 70 percent of large-scale investments in IT-enabled change are wasted, challenged, or fail to bring a return to their enterprise. All of this points to the need for strong systems of enterprise IT governance. Rather than arguing which is the correct definition of IT governance, enterprise senior managers should look at the similarities. In virtually every case, governance involves a mix of the following:

- Control of all aspects of IT work.
- Coordination between different pieces of IT-related work—such as new systems development and IT infrastructure support.
- Measurement of the outcomes of IT systems and processes.
- Compliance with internal IT policies or regulations.
- Justification of the spending for all IT resources.
- IT and enterprise-wide accountability and transparency.
- Strong connections with the needs of IT customers, the broader enterprise, and other stakeholders.

Many of these IT governance issues concern the qualities of IT systems themselves, including newer technology issues, legacy systems using old technologies, security, documentation, and many other areas. Tackling these IT governance issues is not primarily a technical problem but a management issue.

A very general theme of the IT governance issues in this chapter and others going forward is that an enterprise's IT resources and capabilities can no longer be something the business side of the enterprise doesn't understand, and also that IT must understand the business and its needs. Major IT issues should be an issue for board-level executives, even though because of the technical nature of IT some key decisions may be left to IT professionals. IT governance implies a system in which all stakeholders, including the board, internal customers, and related areas such as finance have the necessary input into the decision-making process.

The chapters following discuss many aspects and considerations of IT governance. They will generally focus on enterprise risk issues, IT governance issues, legislative and regulatory issues, security issues, and internal as well as external threats impacting IT governance.

All of the IT governance objectives fit into an overall model, as shown in Exhibit 2.4. IT governance is bounded by performance management, strategic alignment, risk management, and value delivery concepts. In order to implement these, there is a need for strong policy and compliance practices, performance and risk management processes, and an overall understanding of appropriate value delivery. Exhibit 2.4 shows these concepts at a high level, but they will be referenced further in later chapters.

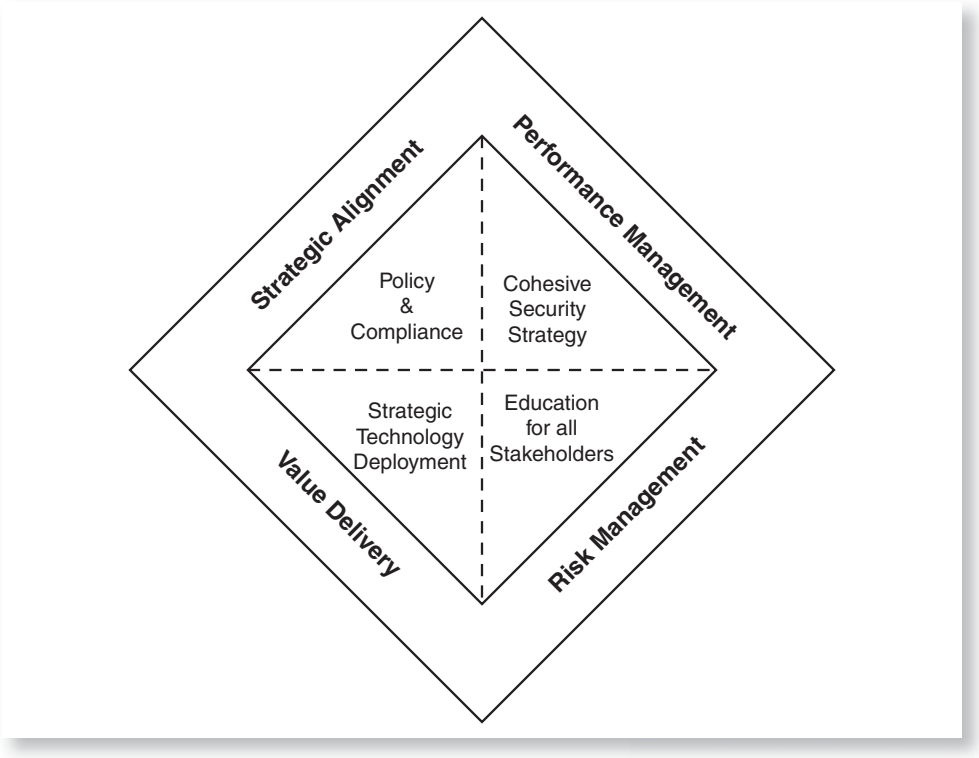

EXHIBIT 2.4 IT Governance Objectives

IT Governance Enterprise Risk Issues

Every enterprise faces a wide range of risks, including enterprise business operations, the business and related market factors, general economic conditions, and an endless list of other enterprise risk factors. Although the objective of this book is not to fully introduce and discuss all aspects of enterprise-wide risk management and what is known as the COSO enterprise risk management (ERM) framework,[5] many aspects of overall enterprise risk management are particularly important for effective IT governance practices. Chapter 4 will provide more information on COSO.

In order to have effective IT governance practices, an enterprise needs to have an effective program for assessing and managing overall risks, significant risks within an enterprise, and specific risks facing IT operations. Exhibit 2.5 outlines some IT governance risk issues and summarizes some effective strategies for managing those risks.

Senior managers are often faced with high or low extremes when accepting and managing many types of IT risks. A systems password to control access to IT resources is a good example here. On one end of things, the not-very-IT-literate manager may want a very simple and easy-to-remember password system, such as just three letters that often become one's initials as well as one digit. A Mary Anne Jones could then just use MAJ1 as her systems password, with the single-digit number changing

EXHIBIT 2.5 IT Governance Risk Issues

Enterprise Risk Requirements	Risk Activation Strategies
Understanding Enterprise Risk Appetite	When faced with alternative potential risks, an enterprise should understand how great and the level of risk to assume. When management is willing to accept riskier ventures, the enterprise is viewed as having a high appetite for risk.
Understanding Risk Acceptance	An enterprise will face many risks, but there should be a clear understanding of what enterprise unit will accept or take responsibility for the risk.
Ensuring the Correct People Are Involved	Organizational unit responsibilities for should be assigned for all identified risks. A unit should recognize that it is responsible for taking appropriate actions if a risk occurs.
Accepting Residual Risks	In an accounting or audit perspective, residual risk is the possibility that an auditor will not catch a material misstatement in a client's financial report and will mistakenly give an unqualified opinion. In a similar sense, management may not recognize the implications of a risk and accept the risk or give things a pass.
Understanding Control Selection Processes	An enterprise needs to understand the costs and implications of various controls that it may establish as a response to various identified risks.
Understanding the Costs of Risk Event Remediation	An enterprise will face many risks, but it should have a clear understanding of the costs to remediate various things if identified risks occur.
Establishing a Clear Risk Mitigation Strategy	An enterprise should have a defined and well-reasoned strategy of what actions to take if an IT-related risk occurs.
Understanding Control Selection Processes	There are many considerations if an IT risk occurs. The enterprise should develop appropriate controls that will correct these risks in an effective manner.

from time to time when passwords change. This is an easy-to-remember—and easily breached—password system.

IT security specialists usually advocate going the other direction in establishing password standards, often a combination of eight or more upper- and lowercase letters, plus numerals and special characters, that all require periodic revision. This can create a much more secure atmosphere, except that many may have trouble recalling these difficult-to-remember passwords and will post them with sticky notes on their computer consoles.

The theme of the risk requirements and strategies outlined in Exhibit 2.5 is that an enterprise needs to have an understanding of the various types of IT risks that it faces as well as the costs and alternative strategies for taking corrective actions if such risk events occur. An important term and concept here is what is called *risk appetite.* That is, how great of a risk is a senior manager and the overall enterprise willing to accept? The individual investor who places his money in AA-rated

corporate bonds has a much lower appetite for risk than does the investor in speculative technology stocks.

An understanding of enterprise risk issues is a requirement for implementing effective IT governance processes. We always need to understand that virtually every area of IT and overall business operations involves the risk of unplanned activities or events occurring. We should always have strategies and processes in place to react appropriately if any of these risks occur.

IT Governance Enterprise Organization Issues

IT governance issues and concerns extend well beyond just the IT department and its resources, and must include many enterprise-wide issues and concerns. We should always consider the IT resource in an enterprise not as just one unique element but a specialized unit or component of the overall enterprise. Some of these governance issues are outlined in Exhibit 2.6.

The message in this exhibit is that although IT management may develop governance processes and procedures affecting their own IT systems and operations, they should always think of them in the much larger context of the overall enterprise. For example, it is too easy to forget that many governance-related actions impact the fiduciary responsibility of the enterprise and its key managers in particular to preserve and enhance the investments of investors at all levels. Failure here could result in civil or even legal actions against enterprise officers. A related consideration here is that an enterprise and its IT operations do not possess an open or unlimited set of resources to take appropriate corrective actions. We must always balance the impact of taking corrective actions against overall enterprise resources.

Exhibit 2.6 also mentions jurisdiction and boundary issues as an IT governance component. Although not too many years ago an enterprise's IT resources existed behind highly secured locked doors and often as a separate facility island from other enterprise operations, we must always think of IT operations as a key component in the continuous process of other enterprise operations. However, we should always remember that boundaries exist, and IT, finance, and other operations should recognize the boundaries between various areas of responsibility when establishing governance processes.

IT Governance Legislative and Regulatory Issues

We began this chapter by providing a summary of some of the key components of SOx, an important item of legislation impacting auditing, financial reporting, and their internal controls. Although a major set of legislative rules, SOx is just one of many major and even more minor legislative and regulatory laws and rules that impact IT governance operations. Some of these cover overall enterprise operations on a national or international level, while others are much more IT-security specific. In other cases, IT governance operations are not impacted by government legislative rules or laws but by professional standards that are voluntary but required to remain at least competitive.

The chapters following will introduce and discuss some of these IT governance legislative and regulatory issues in greater detail. For example, Chapter 10 provides

EXHIBIT 2.6 IT Governance Enterprise Issues

Enterprise-Level Issue	IT Governance Considerations
Corporate Risk-Monitoring Processes	Beyond just identifying the various types and levels of IT and enterprise risks that can impact an enterprise, regular and continuous monitoring processes should be in place to determine the status of these identified risks as well as ongoing action plans to take appropriate actions if the risks occur.
Weak Decision-Making Mechanisms	Beyond just monitoring the status of IT governance risks, management processes should be in place to take appropriate actions in the event of a risk occurring. This is particularly difficult when the planned action involves such matters as shutting down an IT network operation that requires strong and decisive management decisions.
Risk of Personal and Business Records Privacy Exposures	Whether business or financial records or personal data, an enterprise maintains in its records or systems a large amount of data and information that must be protected.
Risks of Ineffective Enforcement and Conflict Resolution	IT governance issues often come to too much or too little corrective action types of considerations when implementing appropriate actions. Strong and regularly tested management processes should be in place.
Lack of Financial Resources Risks	While it is sometimes easy for specialists to develop a risk remediation plan, the enterprise may not have the financial resources to really invoke such a plan.
Failure to Understand Overall Business Responsibilities and Stakeholder Needs Risks	IT operations are too often focused on their own IT infrastructure operations but fail to understand needs and risks for the overall business operaton as well as those of such stakeholders as key vendors or suppliers.
Fiduciary Responsibilities Risks	At all levels, an enterprise and its IT operations always need to remember that they have a duty to protect the assets and investments of their stockholders and lenders.
Boundary and Jurisdiction Identification Risks	All too often, risk monitoring and remediation activities extend beyond just the IT operations to the overall enterprise and to other key stakeholders. There is a need to recognize the jurisdictions and boundaries.

an overview of some of the many IT security rules that impact an enterprise today, and Chapter 11 discusses important elements of the Payment Card Industry Data Security Standard (PCI DSS), an important set of rules impacting any enterprise using credit cards in its business operations. On a different level, Chapter 7 introduces some of the international standards, such as ISO 38500 on IT governance, that are not legislative rules but compliance standards that an astute enterprise should follow.

Legislative and regulatory rules and issues are important components of effective IT governance processes. Enterprise management should monitor these rules and take steps to assure their compliance.

EXHIBIT 2.7 IT Governance Security Issues

IT Security Issues	IT Governance Activities
Security Policy and Procedure Risks	An enterprise should have strong procedures in place to detect and prevent IT security breaches and intrusions. There also should be specialized and skilled staff on board to monitor IT security and to take corrective actions where appropriate.
Business Continuity Planning Issues	Processes should be in place to restore operations in the event of an unexpected disruption in systems and IT operations. These systems should be fully tested and kept current to reflect changes in enterprise operations.
MalWare Risks	Management should recognize that all systems today are subject to an ever-evolving wide range of malicious threats that have the ability to avoid detection and mutate themselves once launched.
Requirements for Effective Intrusion Detection and Security Monitoring Tools	An enterprise should install the appropriate tools to monitor all aspects of IT security, both internally and externally, and to take effective remedial actions when required.
IT Asset Classification Risks	All IT hardware and software assets should be appropriately identified as to their relative security vulnerabilities with corrective action plans tested, implemented, and in place.
Security Monitoring Risks	Tools should be in place to monitor all aspects of IT security and to initiate appropriate actions when any security attacks or breaches are identified.
Encryption Policy and Management Risks	Effective encryption policies should be installed and used where appropriate to improve IT governance practices.
Stakeholder IT Security Risks	Policies and training tools should be in place to ensure that all involved enterprise stakeholders follow appropriate IT security procedures.

IT Governance Security Issues

Because enterprise IT operations are connected both internally and to outsiders through the Internet and many other data connections, security matters are major IT governance issues. Many IT consumers and users recognize that their systems and data are vulnerable to a wide range of outside intruders whose interests range from just disrupting someone's IT operations to sabotaging systems and data for profit or gain. Effective IT security controls are an important element of IT governance.

Today's business executive should have a high-level general understanding of the more significant security issues that are important for effective IT governance. Although

there are many and varied issues here, a business manager should understand IT security threats and risks but should seek specialized technical help within the enterprise to more effectively implement the types of IT governance security processes outlined in Exhibit 2.7.

IT Governance Internal, External Threats

In addition to more specific IT governance issues, an enterprise faces a wide range of internal and external security threats. The external threats can range from such matters as terrorist attacks to foreign government espionage to cloud computing risks and more. While we will discuss some cloud computing IT threats in Chapter 9, an enterprise today faces a wide range of external threats to its IT resources and general business operations. Today's business executive should make certain that appropriate monitoring tools have been established along with skilled people to monitor such threats and take appropriate corrective actions.

IT governance internal threat processes can often be better monitored and controlled. While we never know when some totally unexpected intruder will attack our IT systems, we can reduce the risks of internal threats by establishing strong internal policies and procedures covering many of those discussed in this chapter as well as building a strong team organization where all stakeholders are aware of their roles, responsibilities, and management expectations.

As outlined in this chapter, IT governance is a broad area that covers many areas of enterprise operations and goes well beyond just the IT department. It is much more than the current hot-topic buzzword. Today's enterprise senior executives should work with the IT staff and their security specialists as well as internal auditors to develop strong IT governance practices. The chapters following will provide more background and discussion about implementing effective IT governance practices.

NOTES

1. While we are presenting only a high-level summary of SOx requirements, Robert Moeller, *Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL* (Hoboken, NJ: John Wiley & Sons, 2008), provides much more information.
2. As a public document, the text of the law can be found in many Web locations. One source is http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf.
3. A principle of law: Even if a technical violation of a law appears to exist according to the letter of the law, if the effect is too small to be of consequence, the violation of the law will not be considered as a sufficient cause of action, whether in civil or criminal proceedings.
4. Steve Crutchley, "IT Governance Helping Business Survival," www.slideshare.net/khanyasmin/it-governance-consult2comply.
5. For more information on enterprise risk management and COSO ERM, see Robert Moeller's *COSO Enterprise Risk Management*, 2nd ed. (Hoboken, NJ: John Wiley & Sons, 2011).

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER THREE

Enterprise Governance and GRC Tools

ALL BUSINESSES, AND PUBLICLY TRADED CORPORATIONS in particular, have faced governance needs and requirements issues going back to their earliest days. For many enterprises, senior management often initially took the lead in setting business compliance rules and policies for its employees and others to follow. While this worked with many smaller single proprietorships or in the tightly centralized corporations of eras past, many of today's larger multiunit enterprises need broad-based facilities for setting rules and procedures—they need efficient and effective governance processes.

Life would be easier for those same enterprises if they just had to rely on strong central leadership, such as a dominant chief executive officer (CEO), to authorize and direct implementation of any required governance rules. However, enterprises today at any location or size are faced with ever-increasing sets of rules and procedures ranging from local police and public safety ordinances to state, national, and sometimes international government-issued rules and laws as well as some broad professional rules. An enterprise must comply with these laws and regulations on a whole series of levels, and its compliance failures can potentially result in a variety of penalties. Every enterprise needs processes to ensure that it is operating in compliance with the appropriate laws and regulations.

An enterprise always faces risks that it will misinterpret rules or be found in violation of one or another of these multiple laws and regulations. There are also risks that an enterprise's own established governance rules will not achieve the desired results or that the enterprise may face some outside event beyond its control, such as a significant economic downturn, a terrorist attack or act of war that impacts its sphere of operations, or a fire in a major facility. There is a need to understand and manage all of these risks on an overall enterprise level.

While enterprises have always been concerned with various governance, risk, and compliance issues, the major theme of this book has brought all three of these concerns together in an IT context and into what are known as GRC principles. While other chapters following discuss such issues as the importance of enterprise governance practices, risk management fundamentals, and corporate governance practices, this chapter looks at the importance of establishing a strong set of enterprise governance, risk, and compliance, or GRC, principles, as an important element of IT governance.

THE ROAD TO EFFECTIVE GRC PRINCIPLES

Business professionals had not even heard about this now increasingly familiar GRC acronym until early in this century. The first letter stands for *governance*, not just for IT governance but for concerns over the entire enterprise. In short, governance means taking care of business, making sure things are done according to an enterprise's standards, regulations, board of directors' decisions, as well as governmental laws and rules. It also means setting forth clearly the stakeholder expectations of what should be done so that all stakeholders are on the same page with regard to how the enterprise is run.

The *R* from GRC is *risk*. Everything we do and all aspects of business operations involve some element of risk. When it comes to an individual running across a freeway or a child playing with matches, it's pretty clear that certain risks should just not be taken. When it comes to business, however, risk factors become a way to both help protect existing asset values and create value by strategically expanding an enterprise or adding new products and services. The concept of risk is even more than just the IT governance risks that we will be exploring in greater detail in the chapters to follow.

Finally, the *C* in GRC is *compliance* with the many laws and directives affecting businesses and citizens today. Sometimes people will also extend that letter to include *controls*, meaning that it is important to put certain controls in place to ensure that compliance is happening. For example, this might mean monitoring a factory's emissions or ensuring that its import and export papers are in order. Or it might just mean establishing good internal accounting controls, and effectively implementing legislative requirements such as the Sarbanes-Oxley (SOx) rules briefly discussed in Chapter 2. Putting it all together, GRC is not just what you have to do to take care of an enterprise but a paradigm to help grow that enterprise in the best possible way.

As stated in our introductory paragraphs, not all enterprises, and corporations in particular, historically have thought of GRC as a combined set of principles. As much as an enterprise might have managed or cared about any of these three areas, they were less often managed together than as separate areas or concerns. Risk management is a classic case here. Enterprises thought of risk management in terms of insurance coverage and managed their risks through an insurance department that often had little to do with other enterprise operations. Similarly, we always had a need to comply with all levels of established procedures, including the rules that were established to help govern the enterprise, but we have not historically combined them to form GRC concepts. *GRC*

is an increasingly recognized term that reflects a new way in which enterprises today are adopting an integrated approach to these aspects of their business.

Going beyond just the acronym, it is important to remember these core disciplines of governance, risk management, and compliance. Each of the disciplines consists of the four basic GRC components: strategy, processes, technology, and people.

Exhibit 3.1 illustrates these GRC concepts. Governance, risk management, and compliance principles should be tightly bound to tie these principles together. The diagram also shows that internal policies are the key factors supporting governance, that external regulations drive compliance principles, and that what we call an enterprise's risk appetite is a key element of risk management.

Risk appetite is a relatively new term for many business and IT professionals. It refers to the amount and type of risk that an organization is prepared to pursue, retain, or take. For example, an investor who speculates in what are often called very risky "penny stocks" has a high appetite for risk, while an investor holding generally safe money market funds has a low appetite for risk. This same analogy can be translated to many enterprise business decisions.

The triangle diagram in Exhibit 3.1 also shows the components of strategy, effective processes, technologies (including IT), and the people in the enterprise to make all of this work. Off to the left side, the exhibit shows that an enterprise requires management attention and support, and that correct ethical behavior, organizational efficiency, and improved effectiveness are key. The sections following discuss each of these GRC components further, and many of these basic components also are discussed in other chapters.

IMPORTANCE OF GRC GOVERNANCE

The three GRC principles that support IT governance should be thought of in terms of one continuous and interconnecting flow of concepts, with neither G, nor R, nor C any more important than the others. While the preponderance of the chapters to follow cover many aspects of IT governance, we start our discussion here with the governance aspect of GRC.

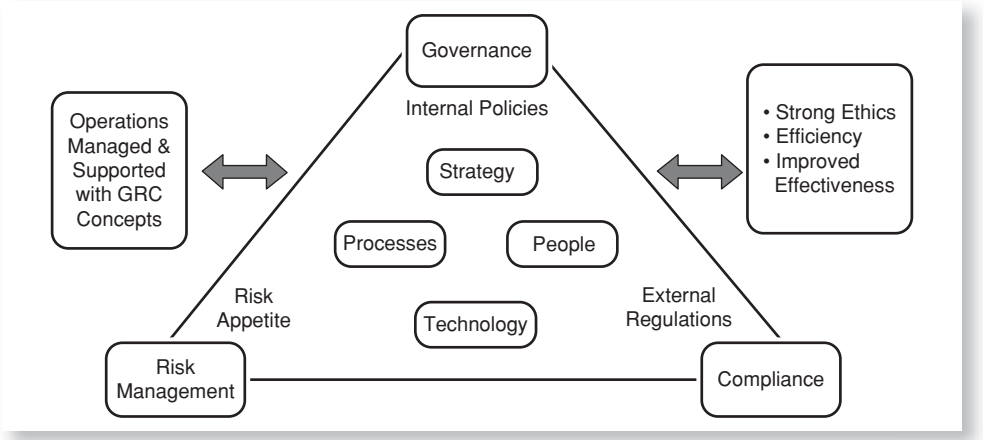

EXHIBIT 3.1 GRC Concepts

Corporate or enterprise governance is a term that refers broadly to the rules, processes, or laws by which businesses are operated, regulated, and controlled. The term can refer to internal factors defined by the officers, stockholders, or constitution of a corporation, as well as to external forces such as consumer groups, clients, and government regulations.

Moving down from senior corporate levels and into many areas of enterprise operations, we can define enterprise governance as the responsibilities and practices exercised by the board, senior executive management, and all levels of senior functional management, with the goals of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly. Governance really refers to the process of establishing rules and procedures within all levels of an enterprise, communicating those rules to appropriate levels of stakeholders, monitoring performance against those rules, and administering rewards and punishments based on the relative performance or compliance with those rules.

A well-defined and well-enforced set of corporate or enterprise governance principles provides a structure that, at least in theory, works for the benefit of everyone concerned by ensuring that the enterprise adheres to accepted ethical standards and best practices as well as to appropriate formal laws, rules, and standards. In recent years, corporate governance has received increased attention because of high-profile scandals involving abuse of corporate power, financial misjudgments, and, in some cases, criminal activity by corporate officers. An integral part of an effective corporate governance regime includes provisions for civil or criminal prosecution of individuals who conduct unethical or illegal acts in the name of the enterprise.

Although we frequently describe all of the concepts of corporate or enterprise governance in a few short paragraphs or a single picture, Exhibit 3.2 shows enterprise governance concepts with an executive group in the center and their interlocking and related responsibilities for establishing controls, a strategic framework, performance, and accountability. The exhibit shows some of the key concepts within each of these responsibility areas. For example, for the strategic framework, there are the elements of corporate planning and business activities, risk management, business continuity, IT and network, and internal audit.

Governance, a key portion of GRC principles, is embedded in many of the chapters on specific IT governance issues going forward, but in particular Chapter 8 on risk management and Chapter 18 on IT governance. Chapter 18 also focuses on IT issues, business strategies, and governance processes.

RISK MANAGEMENT COMPONENT OF GRC

A major objective of this book is to introduce IT governance concepts to today's business executive. A strong set of enterprise-wide GRC principles and components is necessary, and an effective risk management program is a key component of enterprise GRC principles. Chapters 8 and 10 discuss risk management and IT security fundamentals in greater detail, and risk management should be part of the overall enterprise culture from the board of directors and very senior officers down throughout the enterprise. There

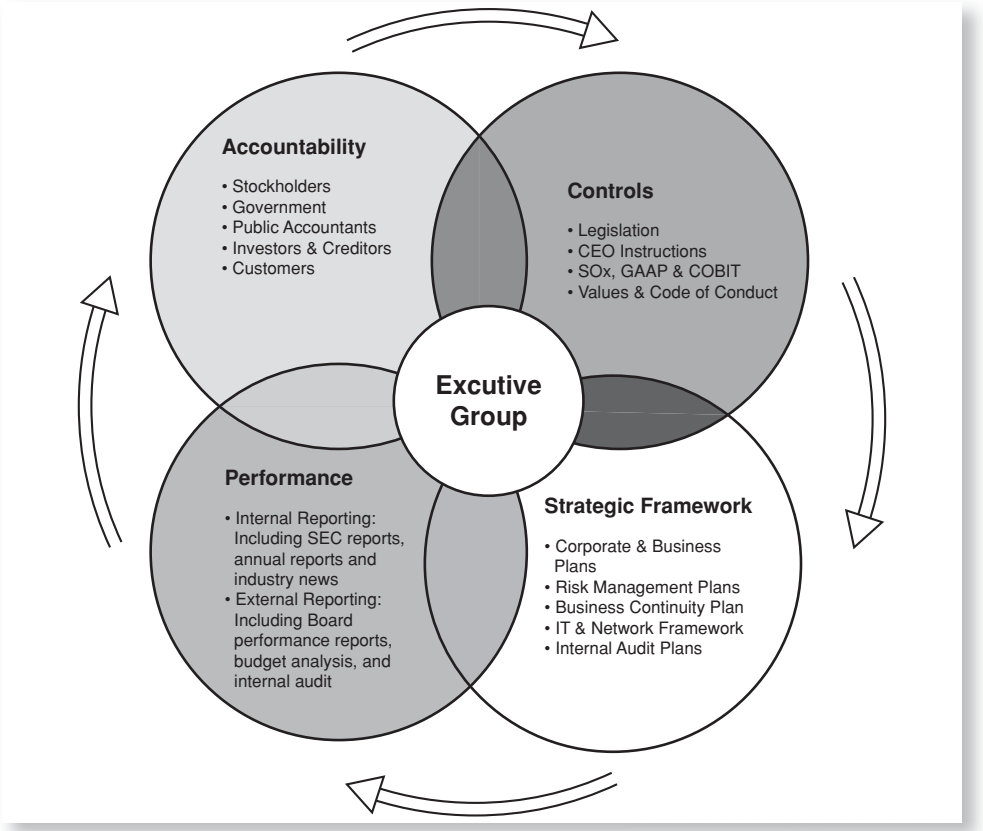

EXHIBIT 3.2 GRC Governance Elements

are four interconnected steps in effective enterprise risk management GRC processes, as shown in Exhibit 3.3 and as follows:

1. **Risk assessment and planning.** An enterprise faces multiple levels of risks, whether global issues ranging from national economic or currency crises to product market competition factors and weather-related disruption at local operations. We cannot plan or identify every type of risk that might impact an enterprise, but there should be an ongoing analysis of the various potential risks an enterprise may face.
2. **Risk identification and analysis.** Rather than just planning for the possibility of some risk event occurring, there is a need for a more detailed analysis on the likelihood of these risks coming to fruition as well as their potential impacts. There is a need to quantify the impacts of the identified risks and to determine mitigation strategies in the event the risk event occurs. Mitigation refers to assessing the best way to manage or eliminate an identified risk. The final factors associated with these risks should also be identified. An identified risk will be much more significant if we can identify the total costs to the enterprise if the identified risk occurs.
3. **Exploiting and developing risk response strategies.** Essentially in parallel with risk identification, an enterprise should develop plans and strategies to return

to normal operations and then recover from a risk event. This may include an analysis of risk-related opportunities. For example, if there is an identified risk that some older factory production equipment may fail, an opportunity may be to abandon that production line and install new equipment using a newer technology and possibly even at a newer or alternative location.

4. **Risk monitoring.** Tools and facilities should be in place to monitor for the identified as well as other newer risks possibly occurring. A smoke detector fire alarm is an example here, although most risk-related monitoring requires a wide series of special reports, established and measurable standards, and a diligent human resources function. The idea is to keep ahead and to reenter these prior risk management steps as necessary.

Risk management should create value and be an integral part of organizational processes. It should be part of the decision-making processes and be tailored in a systematic and structured manner to explicitly address the uncertainties an enterprise faces based on the best available information. In addition, risk management processes should be dynamic, iterative, and responsive to change with the capabilities of continual improvements and enhancements.

GRC AND ENTERPRISE COMPLIANCE

Compliance is the process of adhering to the guidelines or rules established by government agencies, standards groups, or internal corporate policies. Adhering to these compliance-related requirements is a challenge for an enterprise and its related stakeholders because:

- **New regulations are frequently introduced.** Using the United States as an example, a wide swath of agencies, such as the Environmental Protection Agency, regularly issue new rules that may have wide impacts on many enterprises, despite

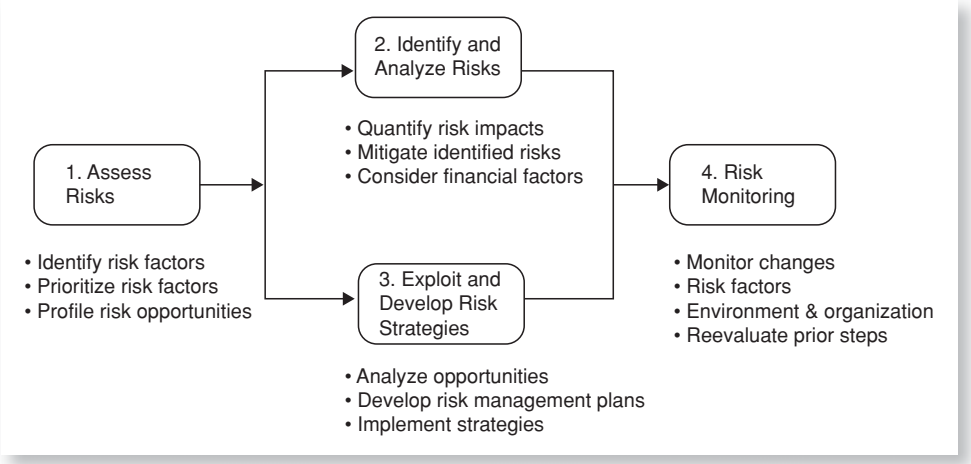

EXHIBIT 3.3 Risk Management Overview

their prime business purposes. Companies have a challenge to monitor these rules and determine which apply to them.

- **Vaguely written regulations often require interpretation.** Again using the United States as an example, in 2010, Congress passed a massive health-care reorganization bill, popularly known as Obamacare, that was drafted by staff members and printed on many thousands of pages covering issues and rules that the legislators who passed the bill never even read, let alone understood. Even today and years from now, we will be looking at these rules and interpreting what they were intended to mean. The 2011 Dodd-Frank financial "reform" bill is a similar example. It is a very complex financial industry regulatory bill with many administrative rules yet to be published as this book goes to press. Enterprise compliance with those types of rules can be very difficult.
- **There is no consensus on best practices for compliance.** Rules are filled with regulations stating such things as, "All transactions must be supported by a receipt." Does such a rule require receipts for transactions less than $1, less than $25, or some other value? There are often no guidelines and everyone seems to have their own interpretations.
- **Multiple regulations often overlap**. U.S. states and local governmental units from different areas frequently issue rules that cover similar areas but have different requirements. These differences are typically eventually resolved in the courts, but compliance until matters are resolved can be a challenge.
- **Regulations are constantly changing.** Regulatory agencies in particular are often constantly changing or reinterpreting their own rules, making strict compliance a challenge.

Enterprise compliance must be viewed as a continuous process, not a one-time project. However, compliance requirements continue to drive business agendas, as enterprises are being held accountable for meeting the myriad mandates specific to their particular markets or areas of operation.

In addition, enterprises might also be required to address cross-industry legislation, such as PCI DSS and other similar rules discussed in Chapter 11, as well as other IT governance and management issues introduced in Chapter 15. Simply stated, the breadth and complexity of these compliance-related laws and regulations have caused challenges for many enterprises over the years. Enterprises need to approach their GRC compliance principles from a more strategic perspective that could help them move beyond simply meeting individual compliance mandates to realizing tangible business benefits from their infrastructure investments as a whole.

The scope of compliance permeates many aspects of enterprise activities and operations. Exhibit 3.4 illustrates some issues an enterprise should consider as it attempts to establish its scope and approach to GRC compliance. An enterprise should not ignore some rules and should always be aware that they exist. Nevertheless, a consistent approach on the use of compliance-driven capabilities and supporting technologies across an enterprise can provide an enterprise with these potential benefits:

- **Flexibility.** One of the difficulties with compliance is that new regulations are introduced by authorizing authorities, and existing regulations are changed on a

frequent basis. By centrally managing compliance initiatives via organization-wide compliance architecture, an enterprise can more quickly adapt to these changes.

- **Reduced total cost of compliance ownership.** Investments can be leveraged across multiple regulations. For example, many regulations specify document retention requirements, which can be met by a single investment in a content database facility and records management system.
- **Competitive advantage.** A broad and consistent compliance architecture can allow an enterprise to better understand and control its business processes, allowing it to respond more quickly and accurately to external or internal compliance pressures. Furthermore, certain regulations may contain tangible business benefits through reduced minimum capital requirements, which could be enabled by an enterprise-wide compliance architecture.

Effective GRC compliance processes help an enterprise to transform its business operations and gain deeper insight and predictability from its business information as it addresses regulatory-driven requirements. Key business drivers here may include the ability to better manage information assets, demonstrate compliance with regulatory and legal obligations, reduce the risk of litigation, reduce cost of storage and discovery, and demonstrate corporate accountability.

EXHIBIT 3.4 Enterprise Considerations for Its Scope of Compliance Activities

Scope of Compliance Area	Area for Considerations
Strategy	■ As an enterprise develops its strategies, it must determine which regulations are more relevant. ■ Compliance sustainability needs to be an integral part of any compliance strategy.
Organization	■ The organizational structure must be established to meet the specific requirements (or intent) of each regulation (e.g., Sarbanes-Oxley recommends the chief executive officer and president be two different people).
Processes	■ Key processes must be documented and practiced. ■ Audits or reviews must take place to ensure documented processes are effectively being used to address compliance/regulation requirements.
Applications and data	■ Applications must be designed, implemented, and continuously tested to support the requirements of each regulation. ■ Data must be properly protected and handled according to each regulation.
Facilities	■ Facilities must be designed and available to meet the needs of each regulation (i.e., some regulations may require records to be readily available at an off-site location).

IMPORTANCE OF EFFECTIVE GRC PRACTICES AND PRINCIPLES

An enterprise needs to adopt strong governance, risk, and compliance processes, with the objective of establishing an effective GRC program. While many of the chapters going forward focus on IT governance processes, we should not forget the overall importance of strong governance, risk, and compliance processes that support both IT governance and other areas of enterprise operations. GRC practices and principles will be folded into all of the chapters going forward, with several devoted to specific risk and governance issues.

As an example, Chapter 15 discusses the importance of implementing integrated systems for the governance and management of IT. It discusses roles and responsibilities for the people and functions needed for effective governance, and outlines approaches for communicating various levels of governance rules. Similarly, Chapter 19 looks at internal audit's role in enterprise IT governance. The chapter outlines a risk assessment and planning approach for an internal audit function to identify its most significant compliance issues, to communicate those compliance rules, and then to monitor its actual compliance performance. The chapter discusses how legal and internal audit can help it to achieve compliance.

While strong IT governance programs are very important to an enterprise, they should be supported by GRC programs of governance, risk management, and overall compliance as well. An enterprise should focus many of its activities strongly on these GRC principles. This chapter has introduced some important high-level enterprise GRC concepts. They should be fundamental components of effective IT governance processes.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

PART TWO

Frameworks to Support Effective IT Governance

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER FOUR

IT Governance and COSO Internal Controls

THE NEED FOR STRONG AND EFFECTIVE INTERNAL CONTROLS is a key element of enterprise IT governance. The need to establish and then assess internal controls has been around since the early days of auditing and has also been an important concern going back to the very early days of information technology (IT) auditing. While there have been many definitions of internal controls in past years, a good general definition for IT governance is that internal control is a process, effected by an entity's board of directors, management, and other personnel, and designed to provide reasonable assurance regarding the achievement of objectives in the effectiveness and efficiency of operations, the reliability of an enterprise's financial reporting, and an enterprise's IT systems and processes, all in compliance with laws and regulations. This definition is similar to the well-recognized definition established by the U.S. Committee of Sponsoring Organizations (COSO), an important internal controls guidance authority that we will be discussing further in this chapter.

Enterprise managers are responsible for implementing and managing internal control processes, while their auditors act as independent parties to both review and perform tests of these internal controls as well as to report to management and other parties whether they are adequate. These internal control reviewers consist of both internal and external auditors, with external auditors in the United States following the auditing standards of the American Institute of Certified Public Accountants (AICPA). Internal auditors generally subscribe to the guidelines of the Institute of Internal Auditors (IIA), their international professional organization introduced in Chapter 19.

Both of these audit organizations have heritages going back to paper-and-pencil days and before today's pervasive use and reliance on IT systems and processes. Over the years, the Information Systems Audit and Control Association (ISACA) and its IT audit professionals also have filled much of the need for effective internal controls.

IT auditors serve in both external and internal audit roles, although perhaps most professionals here serve as internal auditors for their enterprises.

Following up on our Chapter 2 discussion of IT governance and Sarbanes-Oxley Act (SOx) rules, this chapter introduces what is known as the COSO internal control framework and also outlines COSO-related IT governance processes in today's business enterprise. Both COSO internal controls and SOx, discussed in Chapter 2, started as U.S. internal controls guidance rules but have now received worldwide acceptance. They both had their origins as general financial and operations review guidance and are very applicable to IT governance environments as well.

An understanding and use of the COSO internal control framework is important for establishing effective IT governance processes. While these rules and procedures have origins in financial reporting and auditing, in today's IT-centric world, COSO internal controls are important IT governance tools. These are rules that enterprises need to follow in order to assert or attest to regulators that their organizations have effective internal controls in place and that they are operating in compliance with those newer rules.

IMPORTANCE OF EFFECTIVE INTERNAL CONTROLS AND COSO

Internal controls are one of the most important and fundamental concepts that senior managers and business professionals at all levels must understand. The business professional builds and uses internal controls, while auditors review and test the operational, IT, and financial systems and processes with an objective of evaluating their internal controls. Although internal and external auditors have differing objectives, most of our references in this chapter apply to senior managers who have a major responsibility to understand IT governance issues and assess IT-related internal controls.

Although there have been many slightly different definitions of internal controls in the past, the COSO internal control framework discussed in the following sections provides an appropriate definition for the senior manager. It recognizes that internal control extends beyond just accounting and financial matters and includes all enterprise processes. Also, because IT is so embedded in all business processes, IT-related internal controls are a major portion of our overall understanding of internal controls. An enterprise unit or process has good internal controls if it (1) accomplishes its stated mission in an ethical manner, (2) produces accurate and reliable data, (3) complies with applicable laws and enterprise policies, (4) provides for the economical and efficient uses of its resources, and (5) provides for appropriate safeguarding of assets. All members of an enterprise are responsible for the internal controls in their area of operation and for operating them effectively.

Despite or perhaps because of this broad and wide-reaching definition of internal controls, many business professionals have had problems in fully understanding and applying internal control concepts. Looking at our definition a bit differently, the concept of an internal control and supporting control processes goes back to the basic mechanical and paperwork procedures that once frequently existed throughout everyday business operations and life. Control processes are necessary for activities inside and outside today's

enterprise, and many basic concepts and principles are the same no matter where the control is implemented. An automobile provides some basic control examples. When the accelerator—a speed control—is pressed, the automobile goes faster. When the brake—another control—is depressed, the automobile slows or stops. When the steering wheel is turned, the vehicle turns. The driver *controls* the automobile, and all three of these represent the car's basic internal control system. If the driver does not use or improperly uses the accelerator, brake, or steering wheel, the automobile will operate *out of control*.

Expanding this concept just a bit, stop signs, traffic direction signs, and gate crossing barriers all represent external controls for the auto and its driver. The driver is the operator of the automobile-based internal control process or system, but has little decision authority over the message delivered from a traffic light external control.

From an internal control perspective, an enterprise can be compared to our automobile example. There are many enterprise systems and processes at work, such as accounting operations, sales processes, and IT systems. If management does not operate or direct these processes properly, the enterprise may operate out of control. All members of an enterprise should develop an understanding of the appropriate control systems and then determine if they are properly connected to manage the enterprise. These are referred to as the enterprise's *internal control* systems.

Internal Control Standards Background

Although the concept and definition of internal controls is fairly well understood today, this was not true until the late 1980s. Although we often understood the general concept, there had been no consistent agreement among many interested business and accounting professionals of what was meant by "good internal controls." Early definitions that first came from the AICPA and were used by the U.S. Securities and Exchange Commission (SEC) for the Securities Exchange Act of 1934 regulations provide a good starting point. Although there have been changes over the years, the AICPA's first codified standards, called the Statement on Auditing Standards No. 1 (SAS No. 1),[1] defined the practice of financial statement external auditing in the United States for many years. This AICPA definition of internal control has, of course, been subject to changes and reinterpretations over the years. Over this period through the 1970s, there were many internal control definitions released by the SEC and AICPA as well as voluminous interpretations and guidelines developed by the then major external auditing firms.

Things changed in late 1970s and early 1980s, a period when there were many major U.S. enterprise failures due to factors such as high inflation and the resultant high interest rates. There were multiple occurrences where enterprises reported adequate earnings in their audited financial reports, only to suffer a financial collapse shortly after the release of favorable audited financial reports. A few of these failures were caused by fraudulent financial reporting, although many others were due to high inflation or other enterprise instability issues. Nevertheless, several members of the U.S. Congress proposed legislation to "correct" the potential business and audit failures. Bills were drafted and congressional hearings held, but no legislation was passed.

Also in response to these concerns as well as the lack of legislative action, the National Commission on Fraudulent Financial Reporting was formed. It consisted

of five professional organizations: the IIA and AICPA, mentioned previously; the Financial Executive International (FEI), an association of senior financial managers; the American Accounting Association (AAA); and the Institute of Management Accountants (IMA). The AAA is a professional organization for academic accountants, and the IMA is the professional organization for managerial or cost accountants.

The National Commission on Fraudulent Financial Reporting came to be called the Treadway Commission after the name of its chairperson. Its major objectives were to identify the causal factors that allowed fraudulent financial reporting and to make recommendations to reduce their incidence. The Treadway Commission's final report was issued in 1987[2] and included recommendations to management, boards of directors, the public accounting profession, and others. It also called for management reports on the effectiveness of their internal control systems and emphasized key elements in what it felt should be a system of internal controls, including a strong control environment, codes of conduct, a competent and involved audit committee, and a strong internal audit function. The Treadway Commission report again pointed out the lack of a consistent definition of internal control, suggesting that further work was needed. The same Committee of Sponsoring Organizations (COSO) that managed the Treadway report subsequently contracted with outside specialists and launched a project to define internal control. Although it has issued no standards, the Treadway Commission released the COSO internal control framework, discussed in the following sections and referenced throughout this book.

COSO Internal Control Framework

As mentioned, COSO refers to the five professional auditing and accounting organizations that formed a committee to develop this internal control report; its official title is *Integrated Control—Integrated Framework*.[3] Throughout this book, we refer to it as the COSO internal control report or framework. This is in contrast to the COSO enterprise risk management (COSO ERM) resource management framework introduced in Chapter 8. First released in September 1992, the COSO internal control report proposed a common framework for the definition of internal controls, as well as procedures to evaluate those controls. In a very short number of years after its 1992 issuance, the COSO internal control framework has become the recognized worldwide guidance for understanding and establishing effective internal controls in virtually all business systems. The following paragraphs will provide a description of the COSO internal control framework and its use as an IT governance tool for internal controls assessments and evaluations.

Virtually every public corporation has a complex control procedures structure. Following the format of a classic organization chart, there may be levels of senior and middle management in multiple operating units or within different activities. In addition, control procedures may be somewhat different at each of these levels and components. For example, one operating unit may operate in a regulated business environment where its control processes are very structured, while another unit may operate as an entrepreneurial start-up with a far less formal structure. Different levels of management in these enterprises will have different control concern perspectives. The question

"How do you describe your system of internal controls?" might receive different answers from persons in different levels or units in each of these enterprise components.

COSO provides an excellent description of this multidimensional concept of internal controls, defining internal control as follows:

> Internal control is a *process*, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations
> - Reliability of financial reporting
> - Compliance with applicable laws and regulations[4]

Using this very general definition of internal control, COSO uses a three-dimensional model or framework to describe an internal control system in an enterprise. Exhibit 4.1 shows this COSO internal control framework as a three-dimensional model with five levels on the front-facing side and the three major components of internal control—effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations—taking somewhat equal segments of the model with slices across its top. The right-hand side of Exhibit 4.1 shows three segments, but there could be multiples of these depending on the structure of the enterprise.

Each of the COSO internal control framework's front-facing levels, from monitoring on top down to the internal controls environment, will be discussed in greater detail in

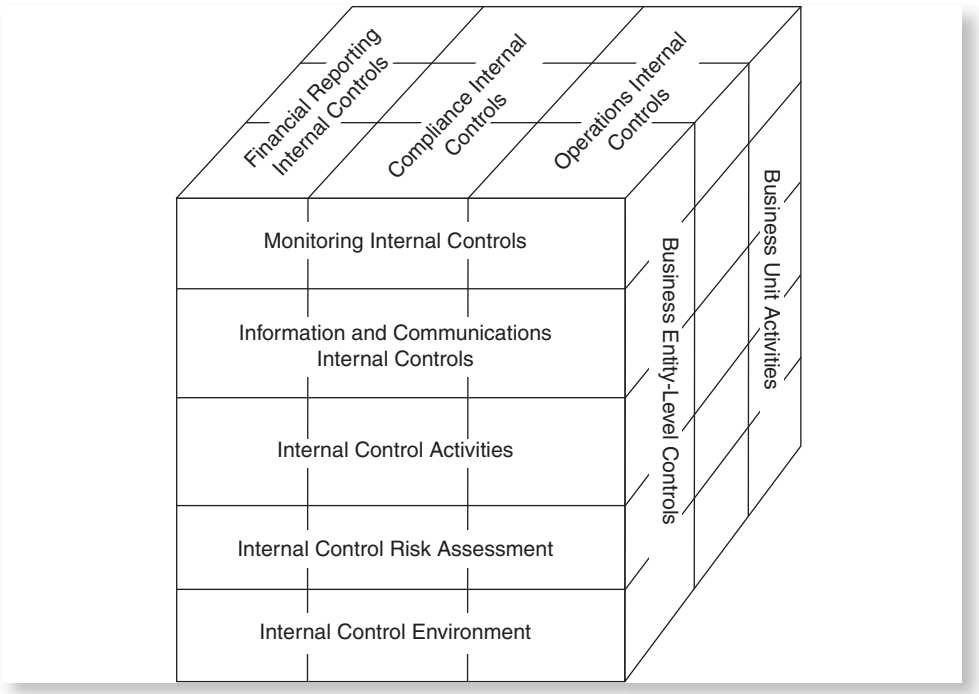

EXHIBIT 4.1 COSO Internal Control Framework

the following sections. The idea here is that when we look at the middle internal control activity layer—such as the period-end financial close—we should consider that control in terms of the business unit or entity or the multiple divisions on the side of the framework where that control has been installed. However, in this three-dimensional model, each control is related to all others in the same row, stack, or column.

The point of the COSO internal control framework is that we should always consider each identified internal control in terms of how it relates to other associated internal control elements in the three-dimensional framework. In our example of end-of-period financial close internal controls, the enterprise should have information and communication links attached to the financial close processes and the control should be monitored. Dropping down a level, there should be risk assessment activities associated with that financial control process, and it should operate in an appropriate internal control environment. Compliance and operations issues may also have factors on the specific control that may function at any level in the enterprise organization.

While the sections that follow will describe COSO internal controls in greater detail, enterprise senior managers should have a strong understanding of the COSO internal control framework and its impact on IT governance. No matter what area is under review, senior managers always should review and consider their internal controls in this type of a multilevel and three-dimensional manner. Starting with the first or bottom front-facing level, the following sections describe the COSO internal control framework in greater detail.

Control Environment

The foundation or bottom level of the COSO internal control framework is what COSO calls the internal control environment. The control environment should be viewed as a foundation for all other components of internal control, and has an influence on each of the three objectives and overall unit and entity activities. The control environment reflects the overall attitude, awareness, and actions by the board of directors, management, and others concerning the importance of internal controls in the enterprise. While there are many fundamental concepts here, each enterprise will have its own unique internal control foundation.

Enterprise history and culture often play a major role in forming this internal control environment. When an enterprise historically has had a strong management emphasis on producing error-free products and when senior management communicates the importance of high-quality products to all levels of the organization, this becomes a major enterprise control environment factor. Messages from the chief executive officer (CEO) or other senior managers are known as the "tone at the top"—management's messages to all stakeholders. However, if senior management has had a reputation of "looking the other way" at policy violations, this same type of negative message will also be similarly communicated to other levels in the enterprise. A positive tone at the top by senior management is a key element of a strong enterprise control environment, whether for IT operations or all other activities.

Senior managers should always try to manage and understand this overall control environment in their organizations. The following paragraphs describe the essential components of the control environment.

INTEGRITY AND ETHICAL VALUES If the enterprise has developed a strong code of conduct that emphasizes integrity and ethical values, and if stakeholders appear to follow that code, all stakeholders will have assurances that the enterprise has a good set of values. A code of ethics or conduct, as discussed in Chapter 20, is an important component of organizational and IT governance. However, even if an enterprise has a strong code of conduct, its principles can often be violated through ignorance rather than by deliberate employee malfeasance. In many instances, employees may not know that they are doing something wrong or may erroneously believe that their actions are in the enterprise's best interests. This ignorance is often caused by poor senior management moral guidance rather than by any employee intent to deceive, and the enterprise's policies and values must be communicated to all organization levels. While there can always be "bad apples" in any enterprise, strong moral messages will encourage everyone to act correctly. The objective should always be to transmit appropriate messages or signals throughout the enterprise.

All stakeholders, and certainly senior managers, should have a good understanding of their enterprise's code of conduct and how it is applied. If the existing code is out of date, if it does not appear to address important ethical issues facing an enterprise, or if the enterprise does not appear to be communicating the code to all stakeholders on a recurring basis, management need to "wake up" and correct this deficiency. While the code of conduct describes the rules for ethical behavior, and while senior management should transmit a proper ethical message throughout the enterprise, other incentives and temptations can erode this overall control environment. Individuals may be tempted to engage in dishonest, illegal, or unethical acts if their enterprise gives them strong incentives or temptations to do so. For example, an enterprise may establish very high, unrealistic performance targets for sales or production quotas. If there are strong rewards for the achievement of these performance goals—or worse, strong threats for missed targets—employees may be encouraged to engage in fraudulent or questionable practices to achieve those goals.

COMMITMENT TO COMPETENCE An enterprise's control environment can be seriously eroded if a significant number of positions are filled with persons lacking required job skills. An enterprise needs to specify the required competence levels for its various job tasks and to translate those requirements into necessary levels of knowledge and skill. By placing the proper people in appropriate jobs and giving adequate training when required, an enterprise is satisfying this important COSO control environment component.

BOARD OF DIRECTORS AND AUDIT COMMITTEE The control environment is very much influenced by the actions of an enterprise's board of directors and its audit committee. An active and independent board is an essential component of the COSO control environment. By setting high-level policies and reviewing overall enterprise conduct, the board and its audit committee have the ultimate responsibility for setting this tone at the top.

MANAGEMENT'S PHILOSOPHY AND OPERATING STYLE The philosophy and operating style of senior management has a considerable influence over an enterprise's control environment. Some top-level managers frequently take significant enterprise-level risks in their new business or product ventures, while others are very cautious or conservative.

Some managers seem to operate by the "seat of their pants," while others insist that everything must be properly approved and documented. Some may take very aggressive approaches in their interpretations of tax and financial reporting rules, while others go by the book. These comments do not necessarily mean that one approach is always good and the other bad.

These management philosophy and operational style considerations are all part of an enterprise's control environment. While no one set of styles and philosophies is best for all enterprises, these factors are important when considering the other components of internal control and IT governance practices in an enterprise.

ORGANIZATIONAL STRUCTURE This internal control component provides a framework for planning, executing, controlling, and monitoring activities to help achieve overall objectives. This control environment factor relates to how functions are managed and organized. While organizational structure is an important aspect of the enterprise's control environment, no one structure provides any preferred internal control environment.

An organizational structure is the manner or approach for individual work efforts to be both assigned and integrated for the achievement of overall goals. Every enterprise needs an effective plan of organization, and a weakness in organization controls can have a pervasive effect throughout the total control environment. Despite clear lines of authority, however, enterprises sometimes have built-in inefficiencies that can become greater as they expand over time, causing control procedures to break down.

ASSIGNMENT OF AUTHORITY AND RESPONSIBILITY This aspect of the control environment is similar to the organization structure component previously discussed. An enterprise's organization structure defines the assignment and integration of its total work effort. The assignment of authority is essentially the way responsibilities are defined in terms of job descriptions and are structured in terms of enterprise charts. Although job assignments can never fully escape some overlapping or joint responsibilities, the more precisely these responsibilities can be stated, the better. The failure to clearly define authority and workplace responsibility will often cause confusion and conflict between individual and group work efforts.

HUMAN RESOURCES POLICIES AND PRACTICES Human resources practices cover personnel hiring, orientation, training, evaluating, counseling, promoting, compensating, and taking appropriate remedial actions. While the human resources function should have adequate published policies and guidance materials, its actual practices send strong messages to employees regarding expected levels of internal control compliance, ethical behavior, and competence. The higher-level employee who openly abuses or ignores a human resources policy quickly sends a message to other levels in the enterprise. The message grows even louder when a lower-level employee is disciplined for violating that same policy while everyone looks the other way at the higher-level violator.

Effective human resources policies and procedures are a critical component in the overall COSO control environment. Messages from the top of strong enterprise structures will accomplish little if the enterprise does not have strong human resources policies and procedures in place.

SUMMARY Just as a strong foundation is essential for a multistory building, the control environment provides the foundation for the other components of internal control. An enterprise that is building a strong internal control structure should give special attention to placing solid foundation bricks in this control environment foundation. The COSO internal control environment does not just require a series of "Do the debits equal the credits?" types of rules but strong overall enterprise-wide effective policies.

Risk Assessment

The next level or layer above the control environment on the COSO internal control framework is risk assessment. An enterprise's ability to achieve its objectives can be at risk due to a variety of internal and external factors. An understanding and management of the risk environment is a basic element of the internal control foundation, and an enterprise should have a process in place to evaluate the potential risks that may impact attainment of its various objectives. This risk assessment component has its focus on internal controls within an enterprise and has a much narrower focus than the COSO ERM enterprise risk management framework and IT governance risk management issues discussed in Chapter 8.

COSO internal control risk assessment should be a forward-looking process that is performed at all levels and for virtually all activities within the enterprise. The COSO internal controls framework describes risk assessment as a three-step process:

1. Estimate the significance of the risk.
2. Assess the likelihood or frequency of the risk occurring.
3. Consider how the risk should be managed and assess what actions must be taken.

This COSO risk assessment process places the responsibility on management to assess whether a risk is significant and, if so, to take appropriate actions. COSO internal controls also emphasize that risk analysis is not a theoretical process but often can be critical to an entity's overall success. As part of its overall assessment of internal control, management should take steps to assess the risks that may impact the overall enterprise as well as the risks over various enterprise activities or entities. A variety of risks, caused by either internal or external sources, may affect the overall enterprise.

The risk assessment element of COSO internal controls is an area where there has been much misunderstanding and confusion because of the similarly named COSO ERM framework discussed in Chapter 8. The risk assessment component of the COSO internal control framework includes risk assessments for *within* an individual enterprise. The COSO ERM framework covers the entire entity and beyond. These are really two separate issues; one is not a replacement for the other.

Control Activities

The next layer up in the COSO internal control framework is called control activities. These are the processes and procedures that help ensure that actions identified to address risks are carried out. Control activities exist at all levels, and in many cases may overlap one another. They are essential elements to building and then establishing effective internal controls in an enterprise. The COSO internal control framework

identifies a series of these activities that are generally classified as manual, IT, or management controls, and they are also described in terms of whether they are preventive, corrective, or detective control activities. While no one set of internal control definitions is correct for all situations, COSO internal controls recommend the following control activities for an enterprise:

- **Top-level reviews.** Senior management should review the results of its performance, contrasting those results with budgets, competitive statistics, and other benchmark measurements. Management actions to follow up on the results of these top-level reviews and to take corrective action represents a control activity.
- **Direct functional or activity management.** Managers at various levels should review operational reports from their control systems and take corrective action as appropriate. Many management systems have exception reports covering these control activities. For example, an IT security system should have a mechanism to report unauthorized access attempts, with a control activity to follow up on these reported events and take appropriate corrective action. Some of these activities link closely with the Information Technology Infrastructure Library best practices discussed in Chapter 6.
- **Information processing.** IT systems often contain controls to check for compliance in certain areas and then report any internal control exceptions. Those exception items should receive corrective action by systems automated procedures, by operational personnel, or by management. Other control activities include controls over the development of new systems or over access to data and program files.
- **Physical controls.** An enterprise should have appropriate controls over its physical assets, including fixtures, inventories, and negotiable securities. An active program of periodic physical inventories represents a major control activity here, and IT as well as internal audit can play a major role in monitoring compliance.
- **Performance indicators.** Management should relate sets of data, both operational and financial, to one another and take appropriate analytical, investigative, or corrective actions. This process represents an important enterprise control activity that can also satisfy financial and operational reporting requirements.
- **Segregation of duties.** Duties should be divided or segregated among different people to reduce the risk of error or inappropriate actions. This is a basic internal control procedure that should be on almost every senior manager's radar screen.

These control activities represent only a small number of the many performed in the normal course of business operations but involve policies establishing what should be done and procedures to implement them. Even though control activities may sometimes be communicated orally, they should be implemented thoughtfully, conscientiously, and consistently. This is a strong message for reviewing such internal control activities. Even though an enterprise may have a published policy covering a given area, there should be established internal control procedures to support that policy. Procedures are of little use unless there is a sharp focus on the condition to which the policy is directed. All too often, an enterprise may establish

an exception report as part of an automated system that receives little more than a cursory review by its recipients. However, depending on the types of conditions reported, those reported exceptions should receive appropriate follow-up actions, which may vary depending on the size of the enterprise and the activity reported in the exception report.

These control activities should be closely related to identify risks from the COSO internal control risk assessment component. Senior managers should always remember that internal control is a process, and appropriate control activities should be installed to address identified risks. Control activities should not be installed just because they seem to be the "right thing to do" even if there are no significant risks in the area where the control activity would be installed. Sometimes there may be control activities in place that perhaps once served some control-risk concern, although the concerns have largely gone away. A control activity should not be discarded because there has been no recent history of control violations, but management needs periodically to reevaluate the associated relative risks. All internal control activities should contribute to the overall control structure, and IT auditors should keep this concept in mind as they review internal controls and make recommendations.

The COSO internal control framework emphasizes that control procedures are needed over all significant IT systems—financial, operational, and compliance-related. COSO internal controls break down information systems controls into the well-recognized general and application controls. General controls apply to much of the information systems function to help ensure adequate control procedures over all applications. A physical security lock on the door to the IT server center is such a general control for all applications running within that facility. IT general controls are discussed in Chapter 6. Application controls, discussed in Chapter 10, are also important IT control areas for evaluating the overall adequacy of internal controls. The COSO internal control framework document concludes with a discussion on the need to consider the impact of evolving technologies whose impact should always be considered when evaluating IT control activities. Due to the rapid introduction of new technologies, what is new today will soon be replaced by something else.

Communications and Information

The COSO internal control framework in Exhibit 4.1 describes most components as layers, one on top of another, starting with the control environment as the foundation. Another way to look at the framework is to think of the COSO internal control framework as a pyramid model with the information and communication components not a horizontal layer but a side element that spans across other components. As important portions of the internal control framework, information and communication are related but are each distinct internal control components. Appropriate information, supported by IT systems, must be communicated up and down the enterprise in a manner and time frame that allows people to carry out their responsibilities. In addition to formal and informal communication systems, enterprises should have effective procedures in place to communicate with internal and external parties. As part of any evaluation of internal controls, there is a need to understand these information and communication flows or processes in the enterprise (see Exhibit 4.2).

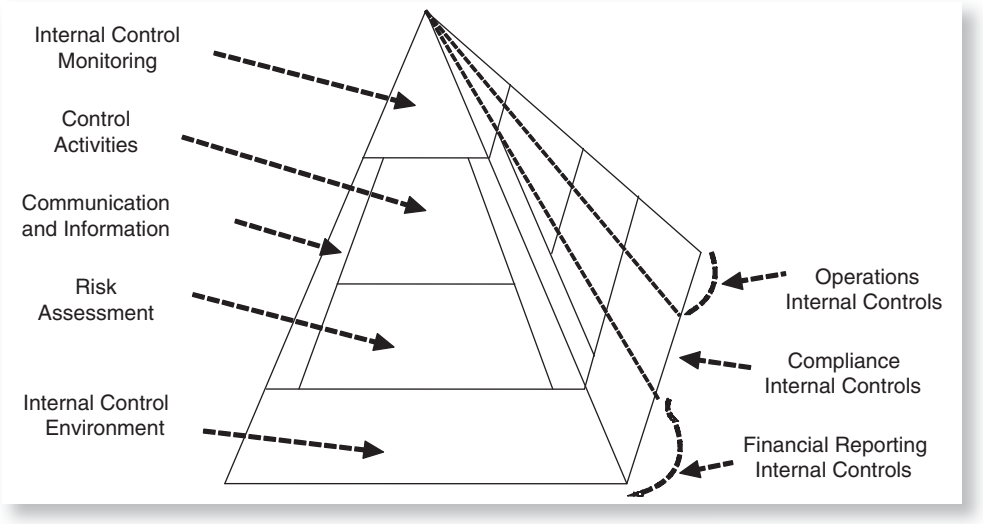

EXHIBIT 4.2 COSO Internal Control Foundation Components

An enterprise needs information at all levels to achieve its operational, financial, and compliance objectives. For example, the enterprise needs information to prepare financial reports that are communicated to outside investors, as well as internal cost and external market preference information to make correct marketing decisions. This information must flow from the top levels of the enterprise on down to lower levels as well as information from the lower levels flowing back to upper levels. COSO internal controls take a broad approach to the concept of an information system, recognizing that these systems can be manual, automated, or even conceptual. Any of these information systems can be either formal or informal. Regular conversations with customers or suppliers can be highly important sources of information and are an informal type of an information system. The effective enterprise should have information systems in place to listen to customer requests or complaints and to forward that customer-initiated information to appropriate personnel.

COSO internal controls also emphasize the importance of keeping information and supporting systems consistent with overall enterprise needs. Information systems adapt to support changes on many levels. IT auditors, for example, often encounter cases where an IT application was implemented years ago to support different needs. Although its controls may have been good, the system may not support the enterprise's current needs. COSO internal controls take a broad view of these types of systems and point to the need to understand both manual processes and automated technologies.

Monitoring

The pyramid view of COSO internal controls in Exhibit 4.2 shows the monitoring component as the capstone, upper level of the COSO internal control components. While internal control systems will work effectively with proper support from management, control procedures, and both information and communication linkages, processes must

be in place to monitor these activities. Monitoring has long been the role of IT and other internal auditors, who perform reviews to assess compliance with established procedures; however, COSO internal controls now take a broader view of monitoring as well and recognize that control procedures and other systems change over time. What appeared to be effective when it was first installed may not be so effective in the future due to changing conditions, new procedures, or other factors.

An enterprise needs to establish a variety of monitoring activities to measure the effectiveness of its internal controls through separate evaluations as well as with ongoing activities to monitor performance and take corrective action when required. Many routine business functions can be characterized as monitoring activities, and COSO gives examples of this important component of internal control:

- **Operating management normal functions.** Normal management reviews over operations and financial reports are an important ongoing monitoring activity, but special attention should be given to reported exceptions and internal control deviations. Internal control is enhanced if reports are reviewed on a regular basis and corrective action initiated for any reported exceptions.
- **Communications from external parties.** External communication monitors, such as a customer complaint telephone number, are important, and the enterprise needs to monitor closely these calls and initiate corrective actions based on these calls when appropriate.
- **Enterprise structure and supervisory activities.** While senior management should always review summary reports and take corrective actions, the first level of supervision often plays an even more significant role in monitoring. Direct supervision of clerical activities, for example, should routinely review and correct lower-level errors and assure improved clerical employee performance. This is also an area in which the importance of an adequate separation of duties is important, and dividing duties between employees allows them to serve as a monitoring check on one another.
- **Physical inventories and asset reconciliation.** Periodic physical inventories, whether of storeroom stock, negotiable securities, or IT assets, are an important monitoring activity. An annual inventory in a retail store, for example, may indicate a significant merchandise loss. A possible reason for this loss could be suspected theft, pointing to the need for better security controls.

These are just a few examples of COSO internal control monitoring activities, the types of procedures that should be in place in many enterprises but are often not thought of as ongoing monitoring activities. Any function or process that reviews enterprise activities on a regular basis and then suggests potential corrective actions should be thought of as a monitoring activity.

While the COSO internal control framework points out the importance of these monitoring activities, it also suggests that "it may be useful to take a fresh look from time to time" at the effectiveness of internal controls through separate evaluations. The frequency and nature of these separate reviews or evaluations will greatly depend on the nature of the enterprise and the significance of the risks it must control.

While management may want to periodically initiate an evaluation of its entire internal controls, most should be initiated to assess specific control areas. These reviews are often initiated when there has been an acquisition, a change in business, or some other significant activity.

COSO also emphasizes that these evaluations may be performed by direct line management through self-assessment reviews. However, responsible management in that area should consider scheduling and performing these self-assessments on a regular basis. This type of internally generated review can point out potential control problems and cause operating management to implement corrective action activities. Because these self-assessment reviews will typically not be as comprehensive as a typical internal audit, follow-up reviews should be launched if potentially significant problems are encountered through limited self-assessment reviews.

Internal Control Evaluation Process The COSO internal control guidance materials outline an evaluation process for reviewing internal controls. Such an evaluator should first develop an understanding of the system design, next test key controls, and then develop conclusions based on the test results. COSO internal controls also mentions *benchmarking*, as an alternative approach. Benchmarking is the process of comparing an enterprise's processes and control procedures with those of peer enterprises. Comparisons are made with similar enterprises or against published industry statistics. This approach is convenient for some measures but filled with dangers in others. For example, it is fairly easy to benchmark the size, staffing levels, and average compensations of a sales function against comparable enterprises in the same general industry; however, the evaluator may encounter difficulties in trying to compare other factors due to the many small differences that make all enterprises unique.

evaluation action plans COSO internal controls recognize that many highly effective procedures are informal and undocumented. Many of these undocumented controls, however, can be tested and evaluated in the same manner as documented ones. While an appropriate level of documentation makes any evaluation of internal control more efficient and facilitates employees' understanding of how the process works, that documentation is not always essential. Any review of an enterprise's internal financial control systems will certainly look for some level of systems documentation as part of the review work. If an existing process is informal, undocumented but recognized as effective, a designated review team will need to prepare an evaluation action documentation to explain how the process works and the nature of its internal controls.

Reporting Internal Control Deficiencies Whether internal control deficiencies are identified through processes in the internal control system itself, through monitoring activities, or other external events, they should be reported to appropriate levels of enterprise management. The key question for any internal controls evaluator is to determine what should be reported given the large body of details that may be encountered, and to whom the reports should be directed. COSO internal controls state that "all internal control deficiencies that can affect the entity's attaining its objectives should be reported to those who can take necessary action." While this COSO internal control statement

initially makes sense, an experienced senior manager realizes that it is often difficult to implement. The modern enterprise, no matter how well organized, will be guilty of a variety of internal control errors or omissions. COSO internal controls suggest that all of these should be identified and reported, and that even seemingly minor errors should be investigated to understand if they were caused by any overall control deficiencies. The published COSO internal control guidance materials use the example of an employee's taking a few dollars from the petty cash fund. This could be viewed as a minor matter due to the small amount of the theft, but it should still be viewed as a control breakdown on several levels.

While the monetary amount may not be significant, COSO internal controls urge that the matter be investigated rather than ignored, since "such apparent condoning personal use of the entity's money might send an unintended message to employees." Prior to SOx, external auditors regularly applied the concept of what was called materiality when performing reviews, and decided that some errors and irregularities were so small that they are not material to the external auditor's overall conclusion. In the first years of SOx compliance reviews with the original AS2 auditing standards, the message from many external auditors was that materiality should not be considered—an error is an error. This approach caused frustration with many managers who wondered why their external auditors were raising issues on what they felt were minor matters. With the current Sarbanes-Oxley rules discussed in Chapter 2, materiality as well as relative risk are now to be considered when evaluating the efficiency and effectiveness of internal controls.

The published COSO internal control guidance concludes by discussing to whom to report internal control deficiencies in the enterprise. One paragraph provides guidance that is useful for evaluations:

> Findings on internal control deficiencies usually should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the enterprise whose activities may be affected. Where findings cut across organizational boundaries, the reporting should cross over as well and be directed to a sufficiently high level to ensure appropriate action.

The enterprise should also develop reporting procedures such that all internal control deficiencies encountered through reviews of ongoing operations should be reported to appropriate levels of the enterprise. Management reporting and monitoring is a highly important aspect of internal controls. Internal audit has a lead role in that process through IT audit reviews, and should also be aware of the need for other monitoring processes when reviewing and evaluating internal controls.

Other Dimensions of the COSO Internal Control Framework

We sometimes forget that the COSO internal control framework is a three-dimensional model, as shown in Exhibit 4.1. In addition to the front-facing

dimension on the model covering control activities, the right-side dimension covers entities or activities, while the top of the framework cube covers the three dimensions of all internal controls:

1. Effectiveness and efficiency of operations.
2. Reliability of financial reporting.
3. Compliance with applicable laws and regulations.

Each of the control areas just discussed—from the control environment to monitoring—should also be considered with respect to those other two dimensions.

In regard to the right-side dimension, internal controls should be installed and evaluated across all units in the enterprise. This does not mean that a control activity, such as an expense approval process, must be identical in all organization units, whether at corporate headquarters or a sales office in a remote geographic location. However, there should be a consistent set of control processes throughout the enterprise with considerations given for the relative risks and scopes of operations. Internal controls should be consistent, but applied appropriately in individual operating units.

The third or top dimension of the COSO internal control framework is even more significant. It says that internal control activities should be installed in all enterprise operating units but with respect to the three factors of internal controls: effectiveness, financial reporting reliability, and regulatory compliance. Looking at internal controls from this three-dimensional viewpoint, there may always be some variations, but under a basic and consistent internal control framework. Using the example of a subsidiary facility in a Central Asian nation far away from U.S. headquarters, country expense approval procedures may be subject to local laws, and other processes may be somewhat different due to communication distances or differences in local IT systems. However, those internal controls should still be implemented in a manner that ensures reliability in financial reporting as results are reported up to corporate headquarters.

An important and very significant concept supporting COSO internal controls is that all internal control considerations must be viewed in terms of the COSO three-dimensional cube. That is, the control must be considered in terms of where it fits in the overall enterprise and its relationship to the three control objective areas just discussed. This concept provides a powerful way of looking at internal controls from a total perspective. The COSO internal control framework continues to be an important standard and set of guidance materials for measuring and evaluating internal controls.

The COSO internal control framework has become the worldwide standard for building and developing effective internal controls. It is a continuous process in each of its three dimensions. On the front-facing side of the model, the monitoring component on top is of little value unless internal control processes are in place all the way down the internal control environment foundation. Similarly, effective internal controls must be installed in all levels of organization units, and each of those controls must be sensitive to the three top-facing internal control elements.

COSO INTERNAL CONTROL SYSTEMS MONITORING GUIDANCE

Extensive guidance materials on the COSO internal control framework have been available, with sources ranging from AICPA auditing standards, to various ISACA materials, and our own additional guidance materials.[5] However, many businesses and not necessarily audit professionals had been seeking more specific guidance on how to implement COSO internal controls in their business operations. A three-volume set of internal control guidance materials was published by COSO in 2009.[6]

All three volumes of this generally excellent set emphasize the importance of monitoring the effectiveness and efficiency of established internal controls. Although our description of the COSO internal control framework, as shown in Exhibit 4.2, shows monitoring as the capstone of the overall process, this COSO study observes that some enterprises have been underutilizing the results of their monitoring activities to develop conclusions about the effectiveness of their internal control processes, sometimes resulting in inefficient or ineffective processes.

This guidance on monitoring internal systems suggests that enterprises implement internal control monitoring processes similar to the manner in which a manufacturing organization monitors the continued effectiveness and efficiency of its manufacturing procedures. The materials suggest that enterprises establish a four-phase monitoring process as shown in Exhibit 4.3. This four-stage approach says that the enterprise should

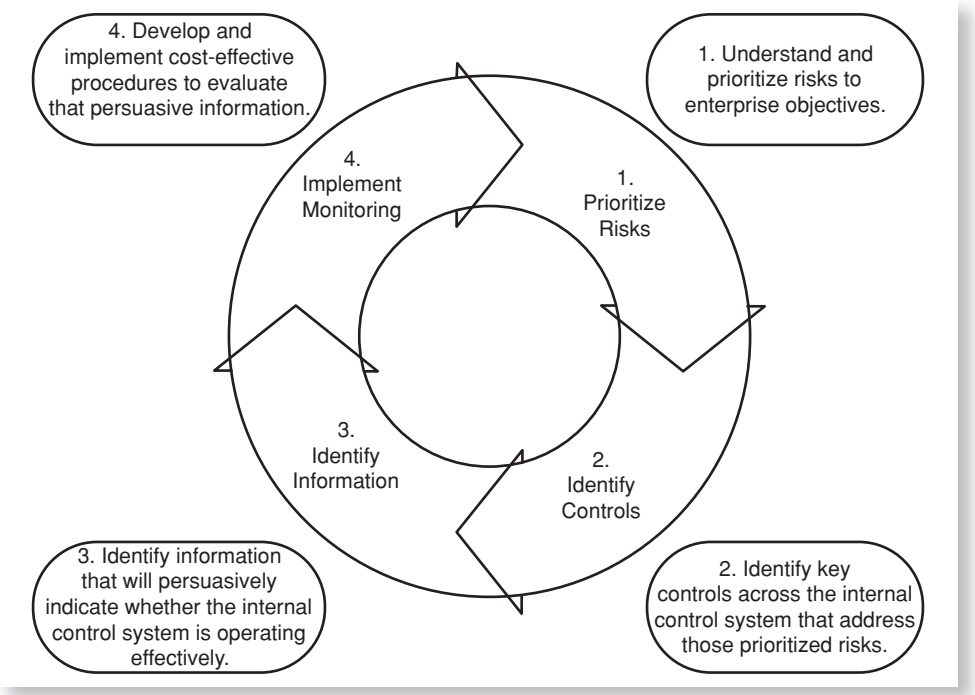
4. Develop and implement cost-effective procedures to evaluate that persuasive information.
1. Understand and prioritize risks to enterprise objectives.
4. Implement Monitoring
1. Prioritize Risks
3. Identify Information
2. Identify Controls
3. Identify information that will persuasively indicate whether the internal control system is operating effectively.
2. Identify key controls across the internal control system that address those prioritized risks.

EXHIBIT 4.3 COSO Monitoring Design and Implementation Process

first prioritize and understand the risks to its organizational objectives, and then identify the controls that address those prioritized risks. The third step is the identification of information that will persuasively indicate that the internal control system is operating effectively. The suggested model calls for implementing cost-effective procedures to evaluate the information gathered through monitoring processes.

WRAPPING IT UP: IMPORTANCE OF COSO INTERNAL CONTROLS

This chapter has introduced the very important COSO internal control framework. Senior managers work in a variety of enterprise environments, and today they will almost always encounter COSO internal control framework requirements. Although this chapter provides only a summary description of COSO internal controls, business executives will encounter these issues when their external auditors review internal controls as part of a financial audit and when their internal auditors review internal controls in a variety of areas.

The COSO internal control framework provides a basis for understanding a wide range of IT governance issues that will be discussed in other chapters going forward. Senior managers should have a general knowledge and understanding of the COSO internal control framework as a basis for understanding enterprise internal controls and related IT governance matters.

NOTES

1. Statement on Auditing Standards No. 1, *Codification of Auditing Standards and Procedures*, AICPA, Professional Standards.
2. *Report of the National Commission on Fraudulent Financial Reporting* (National Commission on Fraudulent Financial Reporting, 1987).
3. *Internal Control—Integrated Framework*. This reference is for the COSO internal controls report that can be ordered through the AICPA at www.cpa2biz.com.
4. AICPA-published COSO internal control standards are described in the Statements on Auditing Standards (SASs) Nos. 103, 105, 106, 107, 109, 110, and 112.
5. See Robert Moeller, *Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL* (Hoboken, NJ: John Wiley & Sons, 2008).
6. *Guidance on Monitoring Internal Control Systems* (COSO, 2009).

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER FIVE

COBIT and the IT Governance Institute

ENTERPRISE PROFESSIONALS AND CERTAINLY SENIOR MANAGERS require the use of a set of standards or a framework to govern their IT governance practices and general internal control procedures. Adherence to such a framework allows senior managers as well as enterprise professionals in their area of expertise to be recognized as specialists in their field of operations. The Committee of Sponsoring Organizations (COSO) internal control framework, as introduced and discussed in Chapter 4, has become an important IT governance tool for evaluating and improving IT governance processes for a wide span of systems and IT processes as well as the internal accounting controls rules under the Sarbanes-Oxley Act (SOx) introduced in Chapter 2. However, some senior managers and their information technology (IT) professionals, in particular, have expressed concerns with using the COSO internal control framework in today's IT-oriented world. The concern had been that the published COSO internal control guidance just does not give enough emphasis on IT tools and processes. For example, the original, 1992-published COSO internal control guidance materials (see Chapter 4) primarily look at IT application internal controls at a very high level, even though there is much more of a need for additional IT-specific internal control guidance in today's world.

A more IT-oriented internal control assessment and guidance framework, called COBIT (*C*ontrol *Ob*jectives for *I*nformation and related *T*echnology), has actually been in place long before SOx, with COBIT first released in 1996. The COBIT framework was initially developed for the internal and external auditors who reviewed computer systems and technology controls (often called IT auditors), but COBIT also has become a preferred tool in many enterprises for complying with SOx Section 404 internal control procedures and related IT governance support. COBIT provides guidance for evaluating and understanding internal controls, with an emphasis on enterprise IT resources. COBIT is not a replacement for the COSO internal control framework but is a different and sometimes preferable way to look at internal controls in today's IT-centric world.

Although originally launched as guidance to help internal and external IT auditor professionals who reviewed IT-related internal controls, COBIT today has evolved into a helpful tool for assessing IT governance and evaluating all internal controls across an enterprise. It provides emphasis and guidance on the linkage of IT with other business resources to deliver overall values to an enterprise today. It is an important tool to help the senior enterprise executive establish effective IT governance practices.

This chapter will provide an executive-level overview of the COBIT framework and many of its key components. The chapter will introduce the newest version, 5.0, which has just been released at the time of our publication. We will introduce other elements of COBIT, such as its board governance guidance and the COBIT-related Val IT framework, an approach to better recognize the value of all IT assets in the enterprise. Val IT addresses assumptions, costs, risks, and outcomes related to a balanced portfolio of IT-enabled business investments. The importance of Val IT will be discussed in Chapter 22. In addition, this chapter will describe the relationship between COBIT objectives and the COSO internal control framework, as discussed in Chapter 4.

Although COBIT had its origins as an IT audit guidance tool, it is much broader today. Today's executives should have a high-level knowledge of the function and purposes of the COBIT framework and should be in a position to question both their IT functions and general financial management operations about an enterprise's use of COBIT in IT governance activities. In addition to the COSO internal control framework, knowledge of COBIT will help a senior manager to better understand the role of IT controls, governance processes, and risks in many enterprise environments.

AN EXECUTIVE'S INTRODUCTION TO COBIT

An unusual or strange-sounding word for many, COBIT is an acronym that is becoming increasingly recognized by auditors, IT professionals, and many enterprise managers. Although it is now abbreviated as COBIT, it was originally written and for many years described as CobiT; in either case the acronym stands for Control Objectives for Information and related Technology. Because of the framework's emphasis on controls and technology, the first and last letters had been capitalized. COBIT is an IT governance internal control framework that is an important support tool for documenting and understanding COSO internal controls and SOx requirements, and for recognizing the value of and risks associated with IT assets in an enterprise. Many members of the internal audit staff may have had at least a general or working knowledge of COBIT, and senior managers throughout the enterprise should also have a general knowledge of COBIT and its importance as an IT governance support tool.

The COBIT standards and framework are issued and regularly updated by the IT Governance Institute (ITGI),[1] and the closely affiliated professional organization, the Information Systems Audit and Control Association (ISACA). ISACA is more focused on IT auditing, while ITGI's emphasis is on research and governance processes. ISACA also manages the Certified IT Auditor (CISA) examination and professional designation as well as other certifications such as the Certified Information Systems Manager (CISM) and the Certified in the Governance of Enterprise IT (CGEIT) designation certification and examination. The Certified Information Security Manager (CISM) certification

targets IT security managers and promotes the advancement of professionals who wish to be recognized for their IT governance–related experience and knowledge.

Many IT and regular internal audit staff members in a typical enterprise are members of ISACA. For nostalgia purposes, ISACA was originally known as the EDP Auditors Association (EDPAA), a professional group that was started in 1967 by internal auditors who felt that their then-professional organization, the Institute of Internal Auditors (IIA), was not giving sufficient attention to the importance of IT systems and technology controls as part of internal audit activities. We have almost forgotten that EDP once stood for electronic data processing, today an almost archaic term for IT. Over time, this professional enterprise broadened its focus and became ISACA.

The EDPAA, originally an upstart IT audit professional organization, began to develop IT audit professional guidance materials shortly after its formation. Just as the EDPAA evolved into the well-respected ISACA and now the ITGI, its original IT audit standards became an excellent set of internal control objectives that evolved into COBIT, now in its 2011 version 5.0 edition.[2] This new edition of the framework was not officially released at the time of our publication, but our comments are based on the final draft releases of this version and the assumption that it will soon become official. With virtually all enterprise processes today tied to IT-related facilities, an understanding of the overall area of IT governance is critical.

The COBIT framework consists of what are called *five principles*, broad and interconnected areas of governance and internal controls, as illustrated in Exhibit 5.1. COBIT's principles are five major areas of emphasis arranged around the important core concept of IT governance:

COBIT Principle 1: An integrated IT framework. COBIT calls for efforts to align IT operations and activities with all other enterprise operations. These include establishing linkages between enterprise business operations and IT plans as well as processes for defining, maintaining, and validating quality and value relationships.

COBIT Principle 2: Stakeholder value drivers. Processes should be in place to ensure that IT and other enterprise operating units deliver promised benefits throughout a delivery cycle and with a strategy that optimizes costs while emphasizing the intrinsic enterprise values of IT and related activities.

COBIT Principle 3: Resources focus on a business context. With an emphasis on IT, there should be optimal investments in, and the proper management of, critical IT resources, applications, information, infrastructure, and people. Effective IT governance depends on this optimization of knowledge and infrastructure.

COBIT Principle 4: Risk management. Management, at all levels, should have a clear understanding of an enterprise's appetite for risk, its compliance requirements, and the impact of significant risks. Both IT and other operations have their own and joint risk management responsibilities that may individually or jointly impact the entire enterprise.

COBIT Principle 5: Performance measurement. Processes should be in place to track and monitor strategy implementation, project completions, resource usage, process performance, and service delivery. IT governance mechanisms should translate implementation strategies into actions and measurements to achieve these goals.

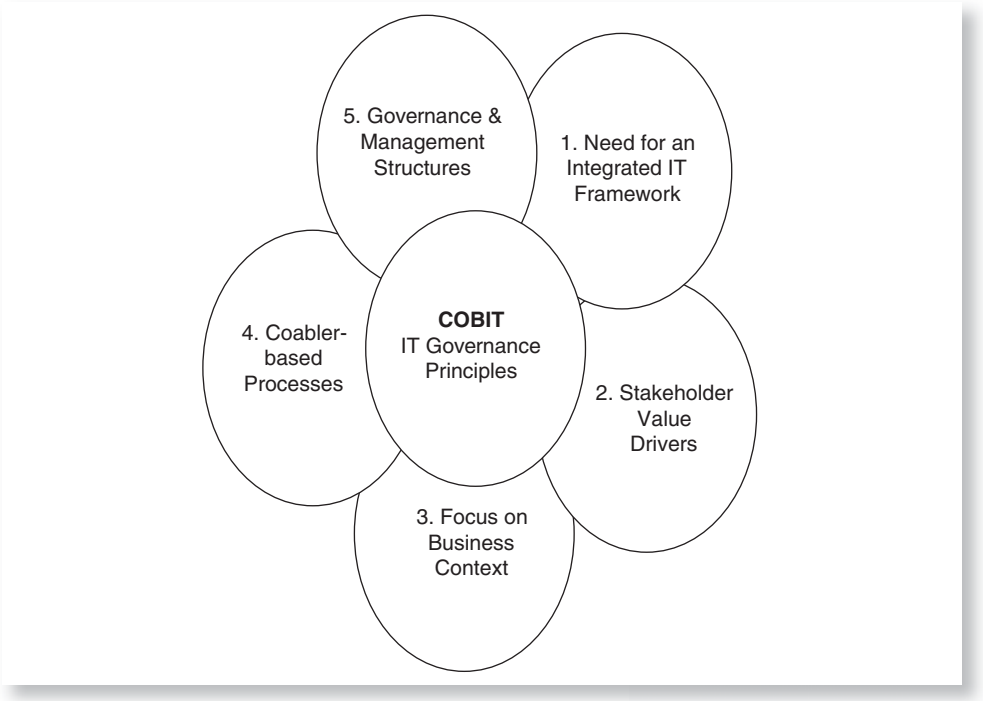
5. Governance & Management Structures
1. Need for an Integrated IT Framework
4. Coabler-based Processes
COBIT
IT Governance Principles
2. Stakeholder Value Drivers
3. Focus on Business Context

EXHIBIT 5.1 COBIT IT Governance Principles

These five COBIT principles or areas of emphasis define the COBIT framework's elements and provide a definition for the key elements of IT governance. The COBIT framework is an effective tool for documenting IT and all other internal controls, and this chapter looks at the framework in the broader perspective of using COBIT to assist in the IT governance processes of management, enterprise, and internal auditing.

The following sections provide an overall description of the COBIT framework, in its current version 5.0 final draft format, and COBIT's key elements that link business with IT goals through key controls and effective measurement metrics. In addition, the chapter will describe the mapping of COBIT standards with the COSO internal control framework, discussed in Chapter 4, the Information Technology Infrastructure Library best practices introduced in Chapter 6, and for overall IT and corporate governance. Elements and key components of IT governance will be discussed as well. The COBIT framework is an effective mechanism for documenting and understanding internal controls and managing IT governance processes at all levels. Although COBIT first started primarily as a set of "IT audit" guidance materials, it is a much more powerful tool today.

THE COBIT FRAMEWORK AND ITS DRIVERS

IT processes and their supporting software applications and hardware devices are key components in any enterprise today. Whether a small retail business, with primary needs to keep track of inventory and pay employees, or a very large "Fortune 50"

corporation, all need a wide set of interconnected and often complex IT processes that are closely tied to their business operations. That is, enterprise business processes and their supporting IT resources should work in a close information-sharing relationship. IT cannot and certainly should not tell business operations what types of IT processes and systems they should consider implementing, but IT provides information to help influence these business decisions. In the very early days of computer systems, IT managers sometimes felt they had lots of answers and promoted systems solutions for their businesses, sometimes with very counterproductive results. However, this relationship has long since changed; IT and business operations generally should have a close mutual relationship of shared requirements and information. An enterprise manager should understand the needs and information-sharing requirements on both sides. IT has responsibilities over a series of other related process areas that are audited by or through established audit guidelines, are measured by a series of performance indicator measures and activities, and are made effective through activity goals. All of these become part of COBIT, an IT governance and control framework defining best practices, governance, and internal control objectives for both IT and business processes.

In addition to the COSO internal control framework and SOx internal controls requirements, this chapter introduces COBIT's new 5.0 version. An enterprise executive might ask, "I think I understand some of the key SOx rules and my enterprise uses COSO internal controls; why should I be concerned about this thing called COBIT, yet another framework?" Our answer here is that COBIT provides *an alternative and sometimes preferable* approach to both define and describe processes that have more of an IT governance emphasis than the pure COSO internal control framework. Information and supporting IT processes often are the most valuable assets for virtually all enterprises today, and management has a major responsibility to safeguard its supporting IT assets, including automated systems. An enterprise executive today needs to understand these information-related processes and the controls that support them. This combination is concerned about the effectiveness and efficiency of their IT resources, processes, and overall business requirements.

The COBIT framework recognizes that information should be considered a key resource for all enterprises, and throughout the whole life cycle of information there is a huge dependency on technology. IT and its related technologies are pervasive in enterprises and they need to be governed and managed in a holistic manner, taking in the full end-to-end business and IT functional areas of responsibility. Through the effective implementation of COBIT framework guidance, an enterprise should achieve increased:

- Value creation through enterprise IT.
- Business user satisfaction with IT engagement and services.
- Compliance with relevant laws, regulations, and policies.

As discussed, the COBIT framework has continued to evolve and improve over the years. Our comments in this chapter are primarily based on COBIT's new 5.0 version, which was still in final draft form as this book was being developed. We will also include some references to the previous and well-recognized 4.1 version of COBIT. The new COBIT 5.0 version is a major improvement and provides excellent support and guidance

for enhancing IT governance processes. Although there may be some final tweaks when the 5.0 version is officially released, many of our descriptions of COBIT will reference this soon-to-be-released final new version. Based on the COBIT IT governance principles shown in Exhibit 5.1, the sections following provide a high-level, executive overview of COBIT and why it is an important IT governance tool.

COBIT PRINCIPLE 1: ESTABLISH AN INTEGRATED IT ARCHITECTURE FRAMEWORK

Architecture describes how we build or the style of our office headquarters, but today it also often refers to an enterprise's IT architecture technology selections. For example, when IT functions moved away from the centralized legacy mainframe computer systems, now many years ago, to networks of smaller server systems, an enterprise IT function would state that it had adopted or implemented "client–server architecture." *Systems architecture* is a term IT functions use to refer to the major hardware or software configurations of their IT resources. COBIT has its own architecture; however, a copy of the current published COBIT 5.0 architecture may scare off non-IT specialists because of the diagram's complexity in its current draft form. Exhibit 5.2 is a simplified diagram of COBIT's version 5.0 architecture components.

Referencing this COBIT architecture and going back to its beginning steps, an important concept here is that COBIT and other IT governance concern processes are driven by their stakeholder needs, ranging from senior management wishing to improve IT governance processes through perhaps IT local management seeking to improve specific application processes. Stakeholders usually are large and differing groups who all have some common as well as sometimes differing interests and concerns with an enterprise's IT governance processes. These needs are presented or delivered to established COBIT processes, with an emphasis on IT governance and value objectives. In addition, since COBIT does not just stand by itself, these needs must be coordinated with other existing enterprise standards, frameworks, and processes.

As illustrated in Exhibit 5.2, these needs flow through what COBIT calls enablers, a series of separate but interconnected processes discussed later in this chapter. The purpose of these enablers is—as the name suggests—to implement and perform governance and management systems processes for enterprise IT. Enablers are broadly defined as specific processes, mechanisms, or anything that can help to achieve the enterprise governance objectives. This includes resources, such as information and people. The COBIT 5.0 framework defines seven categories of enablers:

1. Processes
2. Principles and policies
3. Organizational structures
4. Skills and competences
5. Culture and behavior
6. Service capabilities
7. Information

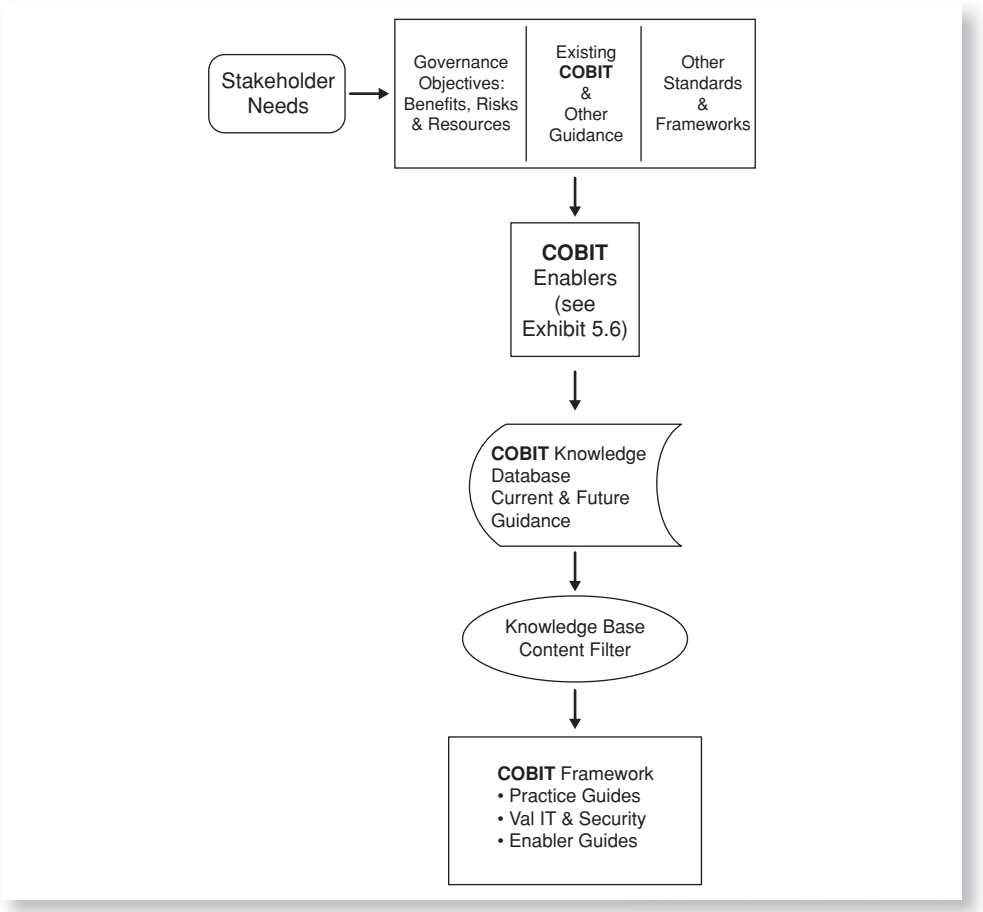
Stakeholder Needs
Governance Objectives: Benefits, Risks & Resources
Existing COBIT & Other Guidance
Other Standards & Frameworks
COBIT Enablers (see Exhibit 5.6)
COBIT Knowledge Database Current & Future Guidance
Knowledge Base Content Filter
COBIT Framework
• Practice Guides
• Val IT & Security
• Enabler Guides

EXHIBIT 5.2 COBIT 5 Simplified General Architecture

These enablers interact in a systemic way, meaning that a governance and management system cannot succeed unless all enablers are addressed, dealt with, and their major interactions understood. We will further discuss these COBIT enablers later in this chapter.

The established enablers then provide support to a COBIT knowledge database, including both current guidance materials and structures for future activities. These then provide support for the overall implementation of COBIT processes that also are supported by a series of product and reference guides. The concept or benefit behind the COBIT architecture is to support the framework's goals by providing to all stakeholders the most complete and up-to-date guidance on the governance and management of enterprise IT. To achieve this benefit, the COBIT architecture includes a wide range of automated and data-related components such as the guidance materials discussed in our other chapters. The purpose and function of these enablers will be discussed in greater detail below.

COBIT is a set guidance materials that supports major elements of IT governance guidance, incorporating many concepts and topics in enterprise governance and management techniques. Enterprises of all sizes around the world have implemented COBIT in its previous 4.1 version. The new COBIT version 5.0 introduces enhancements to reduce IT-related risks and increase confidence in the information provided by IT, to enable clear policy development and good practice for IT management, and to increase the value attained from IT and manage compliance.

COBIT PRINCIPLE 2: STAKEHOLDER VALUE DRIVERS

The business focus of COBIT is achieved through identifying all stakeholders and their needs and determining how they link to governance and management decisions and activities. Perhaps it is best to think of these IT process and operations stakeholders in two groups: internal and external. IT operations and processes are very pervasive, and COBIT's identified internal stakeholders include members of the board of directors, the CEO, chief financial officer (CFO), chief information officer (CIO), business executives, business process owners, business managers, risk managers, security managers, service managers, human resources (HR) managers, internal auditors IT users, IT operations managers, and many others. Each of these will have different expectations and exposures to IT governance issues, but Exhibit 5.3 summarizes some typical COBIT internal stakeholder needs.

This list of stakeholder needs represents some but certainly not all of the many concerns of internal users of IT resources. For example, Exhibit 5.3 contains the need, "How can we use IT resources in the most effective and efficient manner?" A supervisor working in IT operations may think of things in terms of specific network processes, while more senior management will often have much more of a big-picture concern around the same question.

EXHIBIT 5.3 Typical COBIT Internal Stakeholder Needs

- Given IT security, privacy concerns, and other issues, did we address all IT-related risks?
- Are we running an efficient and resilient IT operation?
- How can we better control the cost of IT?
- How can we use IT resources in the most effective and efficient manner?
- What are our most effective and efficient IT equipment sourcing options?
- Do I have enough people to operate and manage IT, and how do I develop and maintain their skills and manage their performance?
- How do we get assurance over the results and performance of IT processes?
- Is the information we are processing well secured?
- How can we improve business agility through a more flexible IT environment?
- Are all levels of management and operations clear on what IT is doing?
- How often do IT projects fail to deliver what they promised?
- How critical is IT to sustaining the enterprise?
- How do we know our business partner's IT and related operations are secure and reliable?
- How do I know the enterprise is compliant with applicable rules and regulations?
- How do we know if the enterprise is maintaining an effective system of internal control?

External stakeholders include business partners, suppliers, shareholders, regulators/government, external users, customers, standardization organizations, external auditors, consultants, and many others concerned with enterprise IT operations and resources. External stakeholder needs include such questions as:

- How do I know if my business partner's operations are secure and reliable?
- How do I know if this enterprise and its organizational units are compliant with applicable rules and regulations?
- How do I know if the enterprise is maintaining an effective system of internal control?

Stakeholder needs are influenced by a number of drivers, including strategy changes, a changing business and regulatory environment, and the evolution of technology. These stakeholder needs materialize in a series of potential expectations, concerns, or requirements; all of these issues relate to one or more of COBIT's three generic governance objectives: benefits realization, risk balancing, and cost optimization.

Enterprises exist to create value for their stakeholders, so the governance objective for any enterprise—commercial or not—is value creation, realizing benefits at an optimal resource cost while optimizing risk. Enterprises have many internal and external stakeholders, and "creating value" means different—and sometimes conflicting—things to each of them. Governance is about negotiating and deciding solutions among different stakeholders' value interests. In consequence, an IT governance system must consider all of these stakeholders when making benefit, resource, and risk assessments and decisions. For each of these value creation components, the question can and should be asked: For whom are the benefits and risks, and which IT resources are required?

COBIT PRINCIPLE 3: FOCUS ON BUSINESS CONTEXT

As mentioned in our earlier comments, COBIT got its start as essentially an IT audit tool, an improved set of recommended processes to review and assess IT internal control procedures. How things have changed over the years! Today, the COBIT framework provides a strong set of guidance materials to help an enterprise improve its IT governance processes, and a core principle of COBIT is its focus on a business context.

COBIT's third key principle emphasizes that business enterprises exist to create value for their stakeholders. There are three COBIT-defined governance value objectives here:

1. Benefits realization
2. Risk optimization
3. Resource optimization

COBIT links each of these three objectives to financial, customer-related, and enterprise-internal enterprise goals. COBIT also defines a set of enterprise financial goals, separated in terms of financial, customer, internal, and learning and growth enterprise goal categories. Exhibit 5.4 shows a summary of these COBIT governance objectives goals mapped to enterprise financial goals in terms of where there is a primary or

EXHIBIT 5.4 COBIT Summary Governance Objectives Mapped to Enterprise Goals

		GOVERNANCE OBJECTIVES		
	ENTERPRISE GOALS	BENEFITS REALIZATION	RISK OPTIMIZATION	RESOURCE OPTIMIZATION
FINANCIAL	1. STAKEHOLDER VALUE OF BUSINESS INVESTMENTS	P		
	2. PORTFOLIO OF COMPETITIVE PRODUCTS AND SERVICES	P		S
	3. MANAGED BUSINESS RISKS (SAFEGUARDING OF ASSETS)		P	S
	4. COMPLIANCE WITH EXTERNAL LAWS AND REGULATIONS		P	
	5. FINANCIAL TRANSPARENCY	P	S	S
CUSTOMER	6. CUSTOMER-ORIENTED SERVICE CULTURE	P		S
	7. BUSINESS SERVICE CONTINUITY AND AVAILABILITY		P	
	8. AGILE RESPONSES TO A CHANGING BUSINESS ENVIRONMENT	P		S
	9. INFORMATION-BASED STRATEGIC DECISION MAKING	P	P	P
	10. OPTIMIZATION OF SERVICE DELIVERY COSTS	P		
INTERNAL	11. OPTIMIZATION OF BUSINESS PROCESS FUNCTIONALITY	P		P
	12. OPTIMIZATION OF BUSINESS PROCESS COSTS	P	P	P
	13. MANAGED BUSINESS CHANGE PROGRAMS	P		S
	14. OPERATIONAL AND STAFF PRODUCTIVITY		P	P
	15. COMPLIANCE WITH INTERNAL POLICIES	S	S	
GROWTH	16. SKILLED AND MOTIVATED PEOPLE	P		P
	17. PRODUCT AND BUSINESS INNOVATION CULTURE	P		

secondary relationship to the COBIT-defined governance value objective. Exhibit 5.5 is a more detailed document for just the financial goal objective. The published COBIT source materials show more detailed relationships for each of the three governance objectives, each mapped to enterprise goals.

This detailed mapping helps to describe COBIT's Principle 3, its focus on a business context. These relationships should help management at all levels and staff members to better understand the relationships and connections between IT processes and both internal and external business activities.

EXHIBIT 5.5 COBIT Detailed Financial Governance Objectives Mapped to Enterprise Goals

		Enterprise Financial Goals				
	ENTERPRISE IT GOALS	Compliance with external laws and regulations	Managed business risks (Safeguarding of assets)	Porfolio of competitive products and services	Stakeholder value of business investments	Financial transparency
		1	2	3	4	5
FINANCIAL	1. STAKEHOLDER VALUE OF BUSINESS INVESTMENTS		S	P	P	
	2. PORTFOLIO OF COMPETITIVE PRODUCTS AND SERVICES	P	S		S	
	3. MANAGED BUSINESS RISKS (SAFEGUARDING OF ASSETS)		S	S	P	
	4. COMPLIANCE WITH EXTERNAL LAWS AND REGULATIONS	S	P			
	5. FINANCIAL TRANSPARENCY			P	P	
CUSTOMER	6. CUSTOMER-ORIENTED SERVICE CULTURE		S		S	
	7. BUSINESS SERVICE CONTINUITY AND AVAILABILITY	S	S	P	P	P
	8. AGILE RESPONSES TO A CHANGING BUSINESS ENVIRONMENT		S	S	S	
	9. INFORMATION-BASED STRATEGIC DECISION MAKING		S	P	S	
	10. OPTIMIZATION OF SERVICE DELIVERY COSTS	P	P			
INTERNAL	11. OPTIMIZATION OF BUSINESS PROCESS FUNCTIONALITY			P	P	
	12. OPTIMIZATION OF BUSINESS PROCESS COSTS		S	S	S	
	13. MANAGED BUSINESS CHANGE PROGRAMS		S	S	P	
	14. OPERATIONAL AND STAFF PRODUCTIVITY	S	S	P	S	
	15. COMPLIANCE WITH INTERNAL POLICIES	S	S			
GROWTH	16. SKILLED AND MOTIVATED PEOPLE		P	S	S	
	17. PRODUCT AND BUSINESS INNOVATION CULTURE			P	S	

COBIT PRINCIPLE 4: GOVERNANCE AND RISK MANAGEMENT ENABLERS

As outlined in our summary description of COBIT's architecture, enablers are key elements in the COBIT governance process. They are the tangible and intangible elements that make something work—in this case, governance and management over enterprise IT. The COBIT 5.0 simplified general architecture in Exhibit 5.2 shows a function called enablers in the center of the overall process. These enablers should be adopted by an enterprise for the governance of IT.

COBIT has defined seven different classes or types of these enablers, as separately illustrated in Exhibit 5.6. To achieve its main objectives, an enterprise must always recognize that it has and manages an interconnected set of these enablers. The general architecture diagram shows seven categories of interconnected enablers. The COBIT-designated enablers are:

1. **Processes.** These are organized sets of practices and activities that achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
2. **Culture, ethics, behavior.** A strong enterprise culture with an emphasis on business ethics and stakeholder behaviors to support those values are often underestimated but important enabler success factors.
3. **Organizational structures.** Activities, policies, and organizational arrangements represent key decision-making vehicles in an organization.
4. **Information.** Critical as a pervasive element throughout any organization, information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
5. **Principles and policies.** These enabler factors are a vehicle to translate desired behavior into practical guidance for day-to-day management.
6. **Skills and competences.** These attributes are linked to people and are required for the successful completion of all activities and for making correct decisions.
7. **Service capabilities.** This enabler includes the infrastructure, technology, and applications that provide the enterprise with information processing and services.

None of these enabler categories exists separately but all need the input of other COBIT-defined enablers to be fully effective. For example, processes need the information enabler, organizational structures need people enablers, and people need skills and behavior. The enablers deliver output to the benefit of other enablers (e.g., processes deliver information, skills, and behavior). Each of these seven COBIT-defined enablers shown in Exhibit 5.6 has its own five specific components:

1. **Enabler stakeholders.** Although we have discussed the importance of stakeholders as drivers of the overall COBIT process, each of the seven enablers here will have its own internal and external stakeholders.

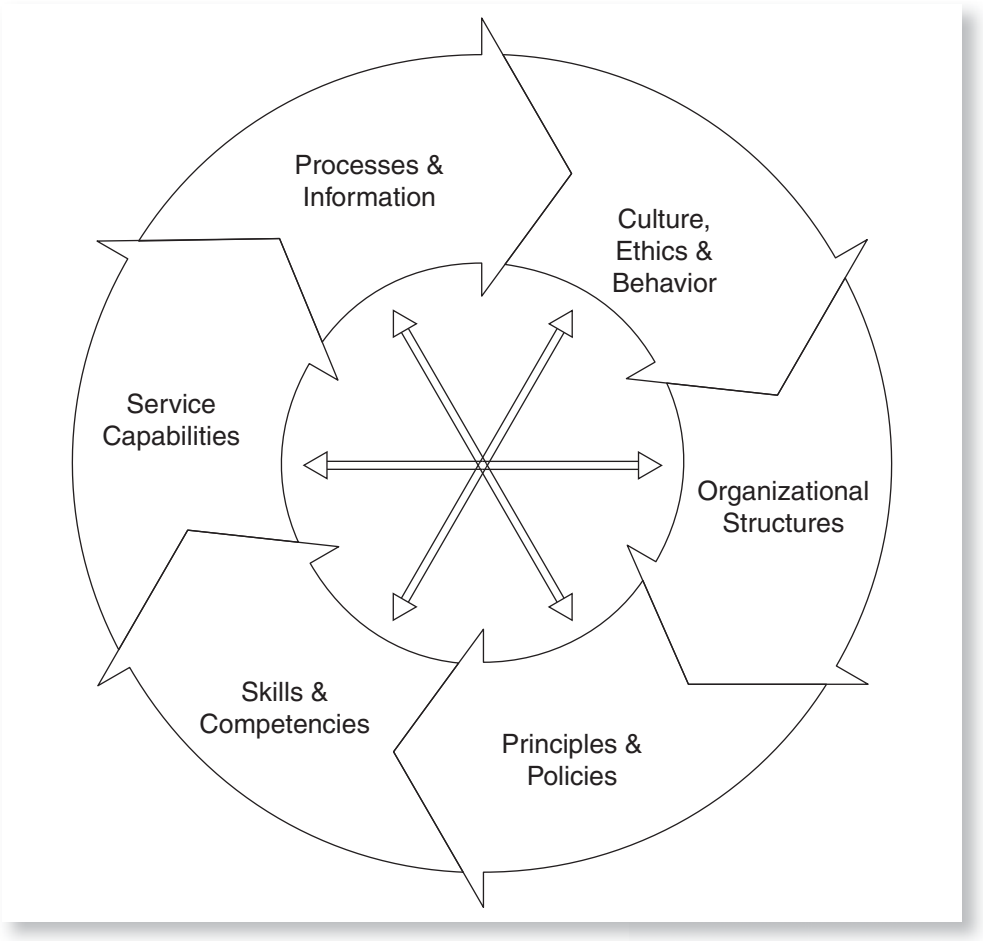

EXHIBIT 5.6 COBIT Classes or Types of Enablers

Processes have internal and external stakeholders, each with its own roles; stakeholders and their responsibility levels should be documented in a manner that represents attributes of the process.

2. **Goals and metrics.** Enabler goals should be defined as a statement describing the desired outcome of a process. An outcome can be an artifact, a significant change of a state, or a significant capability improvement of other processes. They are part of the process goals that support IT-related goals, which in turn support enterprise goals. At each level, metrics should define and measure the extent to which these goals are achieved. Metrics can be defined as a quantifiable entity and should be specific, measurable, actionable, relevant, and timely.

   Goals can be classified in various ways, ranging from economic goals, which are more efficiency-oriented, to quality goals, which are more effectiveness-oriented.

Likewise, there are two types of process metrics: performance metrics, which have a predictive character, indicating the extent to which the process is performing in terms of activities, and outcome metrics, which indicate the extent to which the process really has achieved its goals and purpose.

3. **Enabler life cycles.** Each of these should be supported by plans to establish them and then build, acquire, create, and implement. After their use or operation, the enabler should be periodically monitored and evaluated with an objective update or disposed as required.
4. **Good practices.** Internal and external practices should be installed using tools such as the COBIT framework as well. Good practices enablers have internal and external elements. Both of these include people-skill good practices, including the need for objective skill requirements for each role played by the various stakeholders. This can be described through defined job descriptions for different skill levels in different skill categories. The skill categories correspond with IT-related activities such as telecommunications network management or business analysis.
5. **Enabler attributes.** Each of these will have some unique components that set them apart from other enterprise enablers.

Enabler is a term or concept that was not that common in business operations and processes all that many years ago. The expression first became more common in academic papers on IT issues. We should remember that an enabler is a tool or process that provides measurable capabilities and competencies that enhance, rather than just automate, business processes. They are capabilities, forces, and resources that contribute to the success of an entity, activity, or project. They are worthwhile concepts to add to one's business vocabulary.

COBIT PRINCIPLE 5: GOVERNANCE AND MANAGEMENT PERFORMANCE MEASUREMENT STRUCTURES

COBIT's last key principle focuses on the importance of separate but related concepts of management and governance in an IT-oriented enterprise. The COBIT 5.0 framework makes a clear distinction between governance and management. The two disciplines include different types of activities, require different organizational structures, and serve different purposes. This distinction is a key to COBIT's view of governance and management.

We often forget that *governance*, a popular term in business today, is derived from the Greek verb meaning "to steer." A governance system refers to all the means and mechanisms that enable multiple stakeholders in an enterprise to have an organized say in evaluating conditions and options; setting direction; and monitoring compliance, performance, and progress against plans, to satisfy specific enterprise objectives. This all refers to a major set of steering activities. Means and mechanisms here include frameworks, principles, policies, sponsorship, structures, and decision mechanisms, as well as roles and responsibilities, processes, and practices to set direction and monitor

compliance and performance aligned with the overall objectives. This is a rather large and extensive definition of IT governance, but the chapters following will discuss other issues that support this definition. We should always remember that in most enterprises, governance is the responsibility of the board of directors under the leadership of the CEO and chairperson.

Often differentiated from governance, management entails the judicious use of resources, people, processes, practices, and so on to achieve an identified end. It is the means or instrument by which the governance body achieves a result or objective. Management is responsible for execution within the direction set by the guiding body or unit. Management is about planning, building, organizing, and controlling operational activities to align with the direction set by the governance body.

The COBIT guidance emphasizes that governance and management are different types of activities, with different responsibilities. However, given the role of governance—to evaluate, direct, and monitor—a set of interactions is required between governance and management to result in an efficient and effective governance system. These interactions, using the enabler structure, are then tied to specific internal control review processes, the real strength of the COBIT framework.

PUTTING IT TOGETHER: MATCHING COBIT PROCESSES AND IT GOALS

The published COBIT framework and its supporting materials define a high-level group of processes that set the direction for enterprise business goals and IT resources. Tailored for virtually all types and sizes of enterprises, these are classified in two groups, first as processes for the governance of enterprise IT, and then a second, separate group of processes providing guidance for the management of enterprise IT. Each of these two includes a series of more detailed process categories. For the management of enterprise IT, there are process groups to:

- Align, plan, and organize.
- Build, acquire, and implement.
- Deliver, service, and support.
- Evaluate, direct, and monitor.

Each of these groups then contains more specific COBIT processes. For the build, acquire, and implement group, COBIT guidance is organized in categories of internal control objectives, using the following COBIT-defined coding names:

BAI1—Manage programs and projects
BAI2—Define requirements
BAI3—Identify and build solutions
BAI4—Manage availability and capacity
BAI5—Enable organizational change
BAI6—Manage changes

BAI7—Accept and transition changes
BAI8—Manage knowledge

Similar sets of control objective process categories have been defined for each of the listed process categories. The purpose of the detailed but fairly specific control processes is to help make a business case for the implementation and improvement of the governance and management of IT. Their objective is to recognize both their typical pain points and trigger events, with an overall objective of creating the right environment for IT operations and implementations.

COBIT has defined a set of 17 IT-related goals that can be mapped to each of these processes. These goals also are divided into categories labeled "Corporate," "Customer," "Internal," and "Learning and Growth." These names may change as COBIT moves from its current final draft version, and a category such as "Corporate" does not mean that the guidance applies just to public corporations but rather to the overall enterprise.

Exhibit 5.7 shows the mapping of COBIT's IT-related goals to the factors for two COBIT processes: EDM (evaluate, direct, and monitor) and DSS (deliver, service, and support). This mapping shows how each IT-related goal is supported by a COBIT-related process and is illustrated in Exhibit 5.7 and expressed using a scale where:

- *P* stands for a primary connection between the IT-related goal and the connected COBIT-related process, when there is an important relationship where the designated COBIT process is a primary support for the achievement of an IT-related goal.
- *S* stands for secondary, when there is still a less important relationship, and the COBIT process is a secondary support for the IT-related goal.
- Blank when there is no strong relationship here.

For example, the DSS7 COBIT process to "Manage security" has a strong or primary relationship with the IT-related goal IT called or designated as compliance and support for business-related laws and regulations. That same DSS7 process also has secondary relationships with several other IT goals, such as number 7, the delivery of IT services in line with business requirements.

The COBIT guidance emphasizes that governance and management are different types of activities, each with different responsibilities. However, given governance's steering role—to evaluate, direct, and monitor—a set of interactions is required between governance and management to result in an efficient and effective governance system. These interactions, using the enabler structure, are then tied to specific COBIT internal control review processes, the real strength of the framework.

For many more senior managers, the COBIT framework may seem almost too detailed, with far too complex sets of objectives and goals. Optimal value can be realized from leveraging COBIT only if it is effectively adopted and adapted to suit each enterprise's unique environment. Each implementation approach will also need to address specific challenges, including managing changes to culture and behavior. This chapter has merely touched on the overall structure of COBIT and its current version 5.0.

			IT-related Goals																
			Alignment of IT & business strategy	IT compliance & support for business compliance with laws & regulations	Commitment of executive management for making IT-related decisions	Managed IT-related business risks	Realized benefits from IT-related investments & services portfolio	Transparency of IT costs, benefits & tasks	Delivery of IT services in line with business requirements	Adequate use of applications, information & technology solutions	IT agility	Security of information, IT processing infrastructure & applications	Optimization of IT assets, resources & capabilities	Enablement & support of integrating applications & technology into business processes	Optimization of IT resources & capabilities	Availability of reliable & useful information	IT compliance with internal policies	Competent & motivated IT personnel	Knowledge, expertise & initiatives for business innovation
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	COBIT Processes		Corporate						Customer		Internal							Learning & Growth	
Evaluate, Direct & Monitor	EDM1	Set and maintain the governance framework	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM2	Ensure value optimization	P		S		P	P	P	S			S	S	S	S		S	P
	EDM3	Ensure risk optimization	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM4	Ensure resource optimization	S		S		S	S	S	S	P		P		S			P	S
	EDM5	Ensure stakeholder transparency	S	S	P			P	P						S	S	S		S
Deliver, Service & Support	DSS1	Manage operations		S		P	S		S	S	S	S	P			S	S		
	DSS2	Manage processes		S		P	S		S	S	P			S	S		S	S	
	DSS3	Manage configuration		S		S				S	S	S	S			S			
	DSS4	Manage service requests & incidents				P			S	S		S						S	
	DSS5	Manage problems		S		P	S		S	S	S		P	P	P	P	S		S
	DSS6	Manage continuity	S	S		P	S		P	S	S	S	S			P	S	S	S
	DSS7	Manage security	S	P		P			S	S		P			S	S			
	DSS8	Manage business process controls		S		P			P	S		S		S		S	S	S	S

EXHIBIT 5.7 COBIT Goal and IT Objective Mapping Example

USING COBIT IN A SOx ENVIRONMENT

When SOx first became effective in the United States, there was little guidance on how to implement and manage SOx Section 404 internal control reviews. The Public Company Accounting Oversight Board, introduced in Chapter 2, indicated that it was going to establish some specific standards but initially left enterprises and their external auditors on their own. With its heavy emphasis on high-level IT-oriented internal controls, many enterprises have adopted COBIT as the internal control framework of choice to help achieve SOx compliance.

The SOx Section 404 internal control assessment requirements have highlighted risk-based approaches for evaluating internal controls with an emphasis on the COSO internal control framework, discussed in Chapter 4. COBIT is a powerful alternative internal control assessment framework, particularly in environments with a heavy concentration of IT processes and resources. Both COSO internal controls and COBIT can be described as multidimensional frameworks to describe their internal control environments. Each is similar but with slight differences in classifications and terminology. Exhibit 5.8 shows how the COBIT framework maps to the COSO internal control

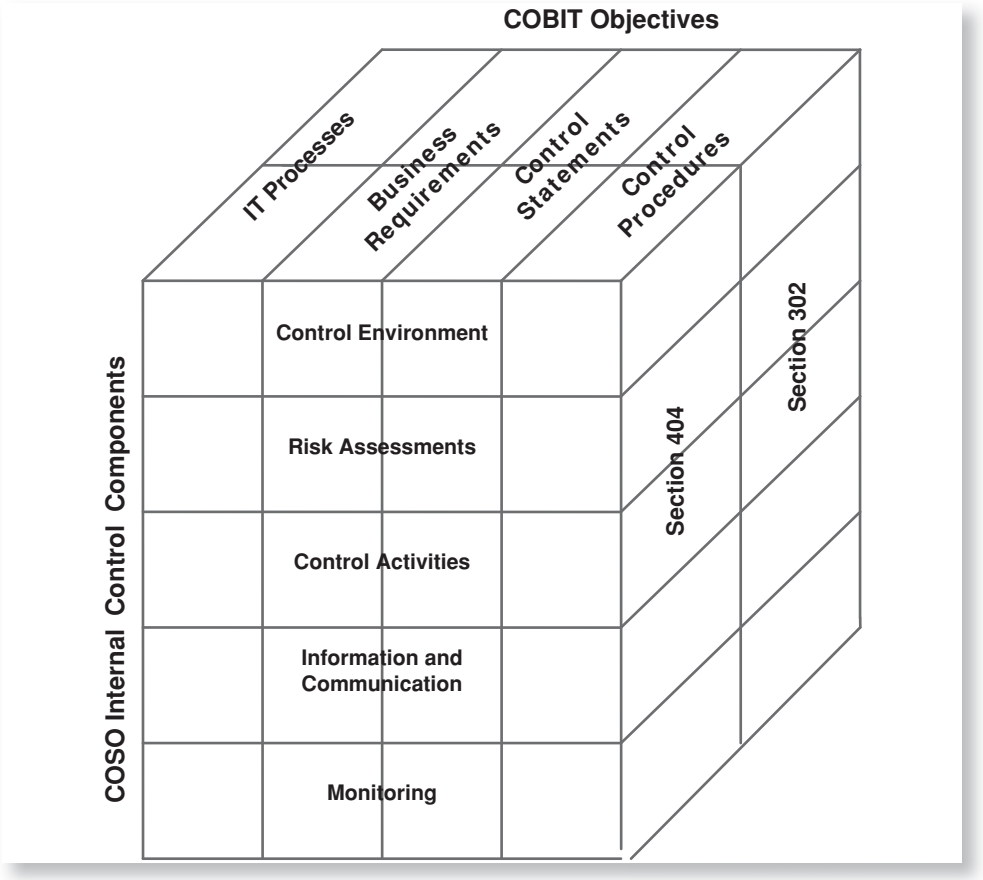

EXHIBIT 5.8 Relationship between COSO Components and COBIT Objectives

model. COBIT's objectives, from planning and enterprise to monitoring and evaluation, can be used to understand and evaluate internal controls through COSO's five internal control components. Whether considering COSO internal controls in general or using COBIT, an analysis of these two that moves through a series of processes from planning to performing risk assessments and on to identifying, documenting, and evaluating key internal controls all will help an enterprise to achieve SOx Section 404 compliance. In addition, with its support of the ITGI professional organization and its widespread international acceptance, COBIT is a living document that is updated from time to time.

With SOx, the increased emphasis on IT governance, and the recognition of the criticality of IT in most internal control decisions, COBIT has gone through multiple revisions up through its current soon-to-be-released 5.0 edition. COBIT's sponsoring IT Governance Institute has been doing an excellent job releasing publications that map the COBIT framework to these other standards.

The full set of COBIT control objectives materials will provide strong support for a management team performing a SOx Section 404 internal control assessment review. While the concepts can be used in any internal control area, the emphasis is on IT applications and processes. For many enterprises, an understanding and assessment of those IT-associated internal controls is a key to achieving SOx compliance. COBIT has been around for some years now, but for too long, many had viewed it as just a specialized IT audit tool and not a more general help for other internal audit and internal controls assessment work. Although COBIT's emphasis continues to be on IT, senior managers should explore this framework as an excellent tool for helping with current and evolving SOx compliance requirements.

COBIT IN PERSPECTIVE

Whether operational, financial, or IT specialists, all enterprise senior managers should have at least a high-level understanding of the COBIT framework. It is a particularly useful and important tool for assessing internal financial controls and overall governance processes in a more IT-oriented environment—the type of environment that we almost always encounter today. The decision to use COBIT in IT governance processes should not be a onetime or individual senior manager's decision. Rather, senior managers as well as their enterprise internal control specialists and internal auditors should develop objectives and take steps to implement the COBIT framework.

COBIT is an elegant—sometimes too elegant—internal control framework and evaluation tool for establishing IT governance processes and assessing internal controls. Perhaps the largest more senior management impediment to its overall use is that COBIT was originally constructed as primarily an IT audit tool. Although the move from ISACA to the ITGI sponsorship has broadened its appeal and focus, there is a very heavy IT focus in many of the published COBIT guidance materials. This certainly scares away some.

The real strength of COBIT is its IT governance focus as described in Exhibit 5.1. That exhibit illustrates the importance of the strategic alliance of business and IT resources with value delivery, resource management, risk management, and performance measurement processes. These allow an enterprise to establish effective IT governance, and

COBIT should help in managing and understanding these concepts. We can expect COBIT published standards and practices to continue to broaden and go beyond just its original "IT audit" special concepts.

NOTES

1. IT Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA), both at Rolling Meadows, IL.
2. *COBIT 5: The Framework Exposure Draft* (Rolling Meadows, IL: IT Governance Institute, 2011).

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER SIX

ITIL and IT Service Management Guidance

IT SERVICE MANAGEMENT (ITSM) is an expression and concept that did not really exist in the earlier days of IT operations for business enterprises. ITSM is the overall discipline or process for managing IT systems centered on the customer's perspective of IT's contribution to the business. ITSM processes operate in deliberate contrast to the technology-centered approaches to IT management from earlier years, and strong ITSM processes are important elements of effective IT governance.

This chapter reviews aspects of ITSM that are important for effective IT governance by introducing senior business professionals to the Information Technology Infrastructure Library (ITIL), a set of internationally recognized best practices covering most aspects of IT operations.

ITIL is the well-recognized abbreviation for the ever-expanding guidance materials first developed in the 1980s by the British government's Office of Government Commerce (OGC). While it was originally an actual library of publications, today it is an independent and regularly updated collection of IT best practices that was first widely recognized by IT operations in the United Kingdom, followed by the European Union (EU), and is now increasingly common in the United States. Just as *IBM* has become a word in itself rather than the acronym for International Business Machines, most professionals today forget ITIL's underlying words.

ITIL is a detailed framework of significant IT best practices, with comprehensive checklists, tasks, procedures, and responsibilities designed to be tailored to any IT function. Dividing key service delivery processes between those covering IT service delivery and those for service support, ITIL has now become the de facto standard for describing many fundamental processes in IT service management, such as configuration or change management. The ITIL framework outlines a series of best practices that are essential for IT governance.

ITIL concepts are important for the effective governance of IT operations in an enterprise. Very different from the early days of enterprise IT systems when the systems developers and IT operations made many major IT-related systems, ITSM calls for the users of this technology to have a much greater role in such overall processes.

ITIL FUNDAMENTALS

ITIL is (or once was) a formal "library" of technical publications, published by the British Office of Government Commerce.[1] The publications and their contents are tightly controlled, similar to the ISO international standards publications discussed in Chapter 7. ITIL provides a framework for the governance of IT and focuses on the continual measurement and improvement of the quality of delivered IT services from both a business and a customer perspective. This focus has been a major factor in ITIL's worldwide success and has contributed to its usage and to the key benefits obtained by enterprises that have deployed ITIL techniques and processes throughout their organizations. Some of these benefits include:

- Increased user and customer satisfaction with the IT services provided.
- Improved service availability, directly leading to potentially increased business profits and revenue.
- Financial savings from reduced rework, lost time, improved resource management and usage.
- Improved time to market for the IT aspects of new products and services.
- Improved decision making and optimized risk for all IT-related processes.

ITIL service delivery best practices cover what is frequently called the IT infrastructure—the supporting processes that allow IT applications to function and deliver their results to systems users. All too often, enterprise management has focused its attention on the application development side of IT processes and ignored important supporting service delivery processes. An enterprise can put massive efforts, for example, into building and implementing a new budget forecasting system, but that budget application will be of little value unless there are good processes in place, such as problem and incident management, to allow the users of this budget forecasting system to report systems difficulties. Also needed are good capacity and availability processes to allow the new application to run as expected. These ITIL processes are all part of the IT infrastructure, and a well-designed and well-controlled application is of little value to its users without such strong service support and delivery processes in place.

While fairly common during recent years elsewhere in the world, ITIL best practices are now also becoming more widely recognized in the United States. The following sections provide an enterprise senior manager overview of some important ITIL service delivery processes. This should give some guidance on how enterprise IT functions should have effective processes in place, such as a help or customer service desk, in important IT process areas. ITIL does not specify particular standards for building and

managing IT controls, but suggests new ways to implement and operate infrastructure general controls that should have already been in place.

ITIL service delivery strategies can be viewed as a continuous activity life cycle, shown as three embedded process activities in Exhibit 6.1: service delivery, service support, and service transition. We will be discussing each of these process activities in the sections following. The concept here is that an ITIL-ready organization should have continual service processes in place that encompass all other service management processes and receive inputs from outside IT customer sources. In the center of these concentric rings is the service strategy process. This core or center process includes the IT organization policies and practices that were described in the COSO control environment element introduced in Chapter 4. Exhibit 6.2 also shows this same service delivery model as a feedback flowchart process.

ITIL processes have traditionally been split between those covering service support and those covering service delivery. Service support processes help make IT applications operate in an efficient and customer-satisfying manner, while service delivery processes improve the efficiency and performance of IT infrastructure elements. There are five ITIL service support best practice processes, ranging from what is called release management, for placing an IT component into production, to incident management, for the orderly reporting of IT problems or events. ITIL service support processes cover good practices for any IT enterprise, ranging from a centralized operation using primarily server or classic legacy mainframe systems as its IT central

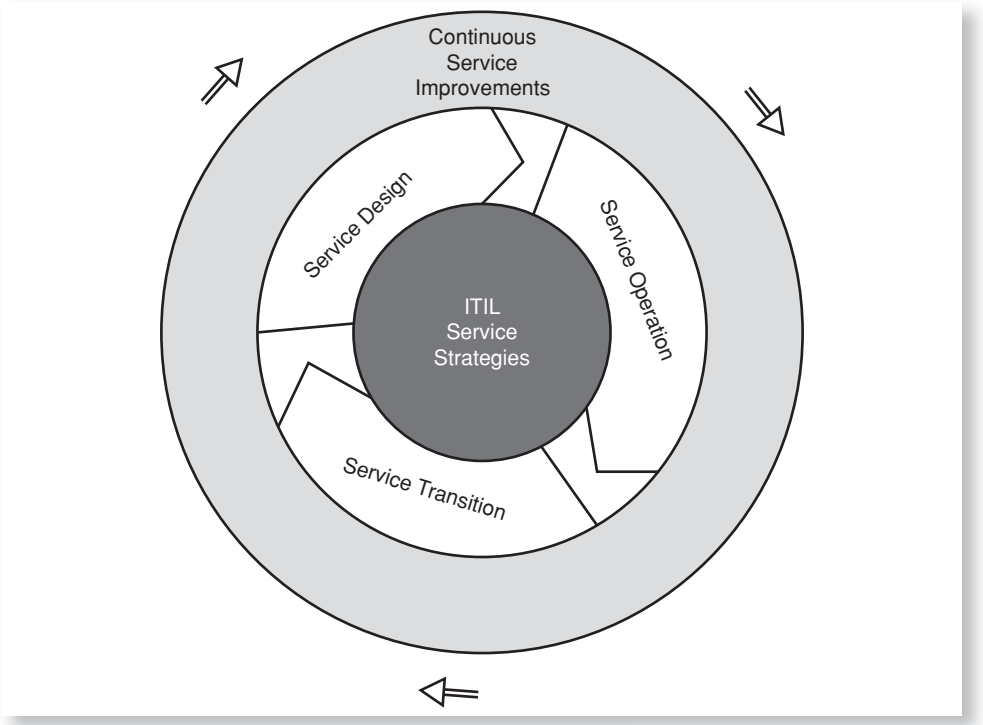

EXHIBIT 6.1 ITIL Continuous Feedback Cycle

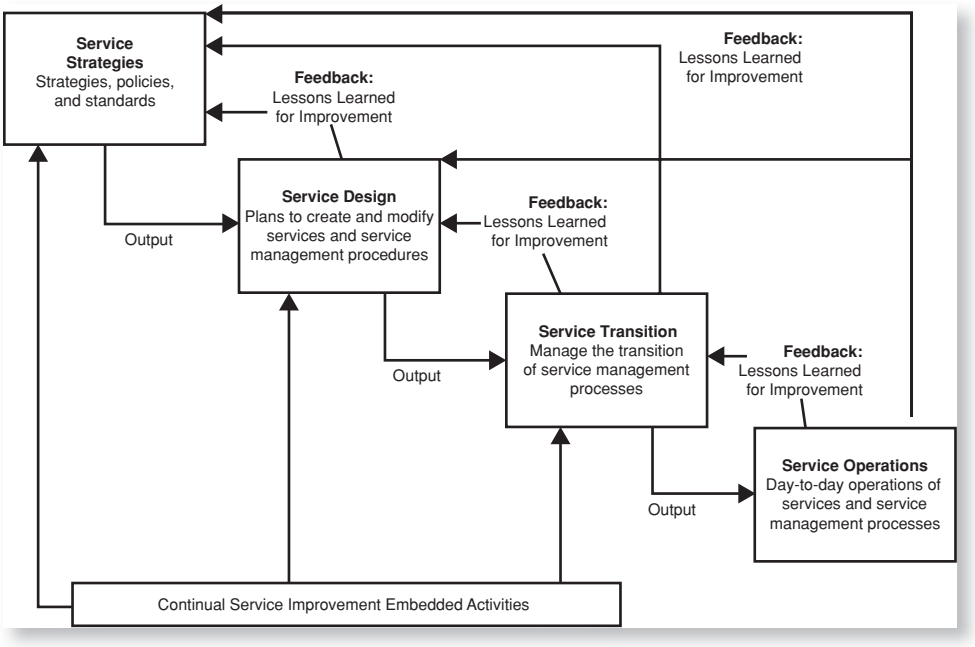
Service Strategies
Strategies, policies, and standards
Feedback: Lessons Learned for Improvement
Feedback: Lessons Learned for Improvement
Service Design
Plans to create and modify services and service management procedures
Output
Feedback: Lessons Learned for Improvement
Service Transition
Manage the transition of service management processes
Output
Feedback: Lessons Learned for Improvement
Service Operations
Day-to-day operations of services and service management processes
Output
Continual Service Improvement Embedded Activities

EXHIBIT 6.2 ITIL Service Feedback Processes

control point to highly distributed client–server operations. Because of the many variations possible in an IT operations function, ITIL does not prescribe the details of "how" to implement service support processes such as configuration or change management. Rather, ITIL suggests good practices and ways to manage inputs and relationships between these processes. There is no order or precedence among each. They can be considered and managed separately, but all of them are somewhat linked to one another. ITIL's service management areas of service delivery and support, along with security management, provide a linkage between the business operations and IT technology and infrastructure management.

Although there are many separate but interrelated elements to ITIL, this chapter will only discuss ITIL's service life cycle components that are more important for effective IT governance processes. These ITIL best practices suggest preferred IT operations approaches to operate IT production systems in a manner that will both promote efficient operations and deliver quality services to the ultimate users or customers of these services. These are particularly useful for performing an assessment and making recommendations in an IT operations area.

When observing and reviewing IT operations internal controls, an often-useful approach is to think of the IT area being reviewed in terms of the separate ITIL processes discussed in the following sections. For example, the ITIL process called incident management, or what has traditionally been called the "help desk," is a facility where systems users or their customers can call in to IT operations with a question or problem. While a help desk function can be very useful, it is often a source of complaint when, for example, a similar problem is called in repeatedly with no evident

efforts to analyze things and initiate a solution to the problem. Going beyond just a casual help desk and thinking of this as an overall process where matters are reported to other supporting processes will improve performance here and the overall quality of IT operations.

ITIL SERVICE STRATEGY COMPONENTS

The upper-left corner of the Exhibit 6.2 diagram of ITIL feedback loop processes shows a function called service strategies. This component describes the ITIL service management policies, strategies, and standards that provide input and direction to the other ITIL service design, transition, and operation processes. Those latter three also provide inputs to service strategies to establish continuous process improvements.

As an IT governance best practice, ITIL suggests that IT management should first assess their service strategy by asking themselves some hard questions about the quality of their IT service function, including:

- Which of our IT services or service offerings are the most distinctive?
- Which of our services are the most profitable for the overall enterprise?
- Which of our customers and stakeholders are the most satisfied?
- Which areas or services are potential problem points or areas for dissatisfaction?
- Which of our activities are most different and effective?

These are not the types of questions that IT management typically asks, whether from management when assessing its IT resources or by senior management or internal auditors. Nevertheless, these are some important questions that IT management should consider when assessing its IT service strategies. The idea is to encourage the enterprise IT function to be more than merely a resource that maintains IT processes but rather one that provides valuable and cost-effective services to the overall enterprise. Exhibit 6.3 is a list of some further questions to help IT to consider and improve their strategic capabilities and offerings.

A multidisciplinary approach would be required to respond to these Exhibit 6.3 questions, because ITIL suggests that the IT organization should work with multiple functions such as operations, finance, quality assurance, and internal audit to better understand and define these key IT strategies for the enterprise. The whole idea is that an IT department or group should decide what they are, in regard to the overall enterprise, and what services they can offer. The latter may result in a service portfolio catalog that defines IT's capabilities and service offerings.

Chapter 5 discussed use of the COBIT framework for establishing effective IT general controls; these are the persuasive types of controls that are installed throughout an enterprise's IT operations to provide protection for all systems and applications. Examples of general controls might be physical locks and other security controls for a hardware server center or a common IT password security system covering all enterprise IT operations. As Chapter 4 on COSO internal controls emphasized, as well as in Chapter 5,

EXHIBIT 6.3 Questions for Developing ITIL Strategic Capabilities

- What IT services should we offer and to whom? That is, do we serve all enterprise units, a limited sample, or outside customers?
- How do we differentiate ourselves from competing alternatives? Outside service providers may offer alternative services, but what are the unique costs or values that make this IT function appear to be a better alternative?
- Has the management team ever seriously considered other alternative IT service functions from outside the enterprise?
- How can we truly create value for our customers? Too often, IT merely handles required services such as month-end financial reports but not information for quick response decisions. IT executives should look to see how they can better service their users.
- How can we make a case for strategic investments? Rather than regularly just submitting budget requests for such matters as software upgrades, does IT carefully evaluate and justify such requests?
- How should we define service quality? Through surveys and collaborative work, do all interested parties recognize quality IT services?
- How do we efficiently allocate our resources across our defined portfolio of offered services?
- How can we resolve conflicting demands for shared services?

poorly implemented or weak IT general controls will impact all IT applications that are part of those IT systems operations.

In today's world of pervasive IT processes and systems, installed throughout the enterprise and ranging from an application to control of a business unit process to the all-pervasive Internet, both involved enterprise management and appropriate personnel should have a strong understanding of IT internal control techniques. Although the lines of separation are sometimes difficult, we can generally think of IT controls on two broad levels: application controls that cover a specific process (such as an accounts payable application to pay invoices from purchases), and what are called general IT controls. This latter category covers many controls that go beyond those discussed in Chapter 4 but are important for all aspects of an enterprise's IT operations.

While the concept of IT general controls goes back to the early days of centralized, mainframe computers, today we often refer to the set of processes that cover all enterprise IT operations as the IT infrastructure. This IT infrastructure will be very different across many enterprises, large and small, due to the relative size of their operations and the overall nature of their business. Because of these many possible variations in the types and sizes of IT systems and facilities that may be needed here, there is really no one single set of right and wrong control procedures here, but an enterprise should establish and implement a set of best practices that will serve as guidance for establishing its own IT general controls.

An important internal control concept here, however, often goes beyond how IT application reports and other IT outputs are delivered to their business users. Every business IT function supports a wide range of ITIL-defined IT service management processes that include such areas as problem management (i.e., how IT resolves issues with

its business users) and configuration management (i.e., how IT keeps track of installed software and equipment versions). IT service management covers a wide range of internal control issues, and rather than specific process rights and wrongs, there are some well-recognized best practices that an enterprise should install. The effective implementation of these ITIL best practices is an important element of overall good IT governance practices.

IT services financial management is an area that is often ignored by both financial and IT management. The ITIL-recommended service management best practices outline a framework here, and the IT function and its management should consider financial management issues when assessing their IT internal control risks and implementing effective IT general controls improvements. Because there is never a single definition for what is known as *best*, some refer to these as just good practices.

Although there are multiple service management strategies identified and described, the financial management for IT services and systems is an important IT governance best practice that is often all but ignored by both enterprise finance and its IT function. This is an area that has been avoided by many IT professionals, who argue that they are not accountants and do not understand accounting-related issues beyond simple budgeting, while the classic financial staff often sees IT services as an issue that is too technical or of no interest beyond basic budgeting. However, this is an important internal control area of potential concern and an ITIL best practice.

In its earlier days, the IT function in most enterprises was operated as a "free" support service with its expenses handled through central management and costs allocated to benefiting users with little attention given to IT-related costs. If a user department wanted some new application, it would pressure management to fund the development work or purchase the software package and add any additional necessary people to manage it. Over time, IT enterprises began to establish charge-back processes for their IT service and support work, but these were too often viewed as a series of "funny money" transactions where no one paid too much attention to the actual costs and the pricing of IT services.

Today, the costs and pricing of IT services should be a much more important consideration. The well-managed IT function should operate more as a business, and ITIL financial management is an important and key ITIL process to help manage the financial controls for that business. The objective of the service strategy financial management process is to suggest guidance for the cost-effective stewardship of the assets and resources used in providing IT services. IT should be able to account fully for its spending on IT services and to attribute these costs of the services delivered to the enterprise's customers. There are three separate subprocesses associated with ITIL financial management:

1. **IT budgeting** is the process of predicting and controlling the spending of money for IT resources. Budgeting consists of a periodic, usually annual, negotiation cycle to set overall budgets along with the ongoing day-to-day monitoring of current budgets. Budgeting ensures that there has been planning and funding for appropriate IT services and that IT operates within this budget during the period. Other business functions will have periodic negotiations with IT to establish expenditure plans and agreed investment programs; these ultimately set the budgets for IT.

2. **IT accounting** is the set of processes that enable IT to account fully for the way its money is spent by customer, service, and activity. IT functions today do not always do a good job in this area. They have a wide variety of external costs, including software, equipment lease agreements, telecommunications costs, and others, but these costs are often not well managed or reported. They have enough data to pay the bills and evaluate some specific area costs, but IT functions often lack the level of detailed accounting such as the cost accounting or activity-based accounting model found in a large manufacturing enterprise.
3. **Charging** is the pricing and billing processes to charge customers for the IT services supplied. This requires sound IT accounting, and needs to be done in a simple, fair, and well-controlled manner. The IT charging process sometimes breaks down in an IT function because the billing reports of IT services are too complex or technical for many customers to understand. IT needs to produce clear, understandable reports of the IT services used such that customers can verify details, understand enough to ask questions regarding service, and negotiate adjustments if necessary.

Financial management for IT supports the service strategy process through these defined costing, pricing, and charging procedures. While generally not operated as a profit center, the financial management process allows both IT and its customers to better think of IT service operations in business terms. The financial management process may allow IT and overall management to make decisions about what, if any, functions should be retained in-house or outsourced to an external provider.

The ITIL financial management process allows accurate cost-benefit analyses of the IT services provided and allows the IT enterprise to set and meet financial targets. It also provides timely reporting to the service level management process, such that customers can understand the charging and pricing methods used. Of all of the ITIL service support and delivery processes, financial management is one ITIL best practice that frequently gets short shrift. IT people have a technical orientation and tend to think of financial management as an *accounting issue.* On the other side of the coin, finance and accounting professionals tend to look at these issues as too technical and beyond such transactions as equipment lease accounting or facility space charges. The costs and prices of IT services are an important IT governance issue.

ITIL SERVICE DESIGN

There are three ITIL service strategy process areas in the IT service life cycle, starting with service design, as shown in Exhibit 6.1. ITIL processes for service design cover areas more closely aligned with the smooth and efficient operation of the overall IT infrastructure. ITIL identifies five aspects of service design:

1. The design of each IT service offered, including their functional requirements, resource needs, and anticipated capabilities.
2. The design of service management systems and tools, often presented through a formal portfolio, for the management and control of these services through their life cycles.

3. The design of IT architectures and management systems necessary to provide the services.
4. The design of processes needed to install, operate, and improve these overall service processes.
5. The design of measurement methods and metrics of the service processes and their component architectures.

What ITIL defines as customer services really says that every IT function installs a lot of customer services, and these offered services should be managed and controlled through appropriate IT governance and best practice techniques. To support efficient service delivery, ITIL has specified a series of specific processes. Some of these, such as the continuity management process, have traditionally been near and dear to the hearts of IT management and its auditors over the years. Others, such as service level agreements (SLAs), that define performance and expectations between IT and its customers are not always well understood or implemented; SLAs are discussed in Chapter 17.

Service Delivery Capacity Management

ITIL capacity management ensures that the capacity of the IT infrastructure is aligned to business needs to maintain the required level of service delivery at an acceptable cost through appropriate levels of capacity. Through gathering business and technical capacity data, this ITIL process should result in a capacity plan to deliver cost-justified IT capacity requirements for the enterprise. In addition to a prime objective to understand an enterprise's IT capacity requirements and to deliver against them, capacity management is responsible for assessing the potential advantages new technologies could have for the enterprise.

The ITIL capacity management process consists of three subprocesses: business, service, and resource capacity management. Business capacity management is a long-term process to ensure that the future business requirements are taken into consideration and then planned and implemented as necessary. Service capacity management is responsible for ensuring that the performance of all current IT services falls within the parameters defined in existing SLAs. Finally, resource capacity management has more of a technical focus and is responsible for the management of the individual components within the IT infrastructure. The multiple inputs to these capacity management subprocesses include:

- SLAs and SLA breaches (as discussed further in Chapter 17)
- Business plans and strategies
- Operational schedules as well as schedule changes
- Application development issues
- Technology constraints and acquisitions
- IT incidents and problems
- Budgets and financial plans

As a result of these multiple inputs, the capacity management process—often under a single designated capacity manager—should manage IT processes, develop

and maintain a formal capacity plan, and ensure that certain capacity records are up to date. In addition, the capacity manager must be involved in evaluating all changes to establish the effect on capacity and performance. This capacity evaluation should happen both when changes are proposed and after they are implemented. Capacity management must pay particular attention to the cumulative effect of changes over a period of time that may cause degraded response times, file storage problems, and excess demand for processing capacity. Other capacity management process responsibilities include some duties of the network systems manager and application development manager. They are responsible for translating the business requirements into the required capacity to be able to meet these requirements and to optimize IT performance.

The implementation of an effective capacity management process offers IT the benefits of an actual overview of the current capacity in place and the ability to plan capacity in advance. Effective capacity management should be able to estimate the impact of new applications or modifications as well as provide cost savings that are in tune with enterprise operations requirements. Proper capacity planning can significantly reduce the overall cost of ownership of an IT system. Although formal capacity planning takes time, internal and external staff resources, and software and hardware tools, the potential losses incurred without capacity planning can be significant. Lost productivity of end users in critical business functions, overpaying for network equipment or services, and the costs of upgrading systems already in production can more than justify the cost of capacity planning. This is an important ITIL process, and IT management should consider the capacity management processes in place when reviewing IT governance processes here.

Chapter 9 contains a further discussion of IT capacity management issues when viewed from the perspective of cloud computing and virtualization. Cloud computing refers to the massive, multiserver IT resources that are provided by an increasing number of major vendors. In an era of ever-more-available cheap storage resources, we tend to think of almost-unlimited IT storage resources. Virtualization is another capacity management and IT governance topic discussed in Chapter 9; it refers to software tools where IT resources are shared in such a manner that we tend to not be concerned about resource limitations in any device. These techniques are changing many approaches, but ITIL capacity management is still an important IT governance concept.

Service Delivery Availability Management

Enterprises today are increasingly dependent on their IT services being available seven days a week and 24 hours a day. In many cases when those IT services are unavailable, the business stops as well. It is therefore vital that an IT function manage and control the availability of its services. This can be accomplished by defining the requirements from the business regarding the availability of the IT services and then matching them with the possibilities of the IT enterprise.

ITIL's availability management best practices depend on multiple inputs, including requirements regarding the availability of the business; information on reliability,

maintainability, recoverability, and serviceability; and information from the other processes, incidents, problems, and achieved service levels. The objectives of the availability management process are to:

- Produce and maintain an appropriate and up-to-date availability plan that reflects the current and future needs of the enterprise.
- Provide service and guidance to all other areas of the enterprise on IT availability–related issues.
- Ensure that service availability achievements meet or exceed targets, by managing service- and resource-related availability performance.
- Assist with the diagnosis and resolution of availability-related incidents and problems.
- Assess the impact of all changes on the availability plan and the performance and capacity of all services and resources.
- Ensure that proactive measures are implemented wherever those actions are cost-justifiable.

Availability management activities can be described as planning, improving, and measuring actions. Planning involves determining the availability requirements to find out if and how IT can meet them. The service level management process, discussed further in Chapter 17, maintains contact with the business and will be able to provide appropriate expectations to availability management. The business may have unrealistic expectations with respect to its IT availability without understanding what this means in real terms. For example, business users may want 99.9 percent availability yet not realize that this will cost five times more than providing only 98 percent availability. It is the responsibility of service level management and the availability management process to manage such expectations.

Exhibit 6.4 shows this availability and costs relationship. It does not cost very much to keep basic lower-availability IT systems running, if that is all the enterprise will receive. IT management should keep this relationship in mind when reviewing controls and making recommendations.

An IT function can either design for "availability" or "recovery." When the business cannot afford a particular service downtime for any length of time, IT will need to build resilience into its infrastructure and ensure that preventative maintenance can be performed to keep services in operation. In many cases building "extra availability" into the infrastructure is an expensive task that can be justified by business needs. Designing for availability is a proactive approach to avoiding downtime in IT services.

When the business can tolerate some downtime of services or a cost justification cannot be made for building additional resilience into the infrastructure, designing for recovery is the appropriate approach. Here, the infrastructure will be designed such that in the event of a service failure, recovery will be "as fast as possible." Designing for recovery is a more reactive management approach for availability. In any event, other ITIL processes such as incident management need to be in place to recover as soon as possible in case of a service interruption.

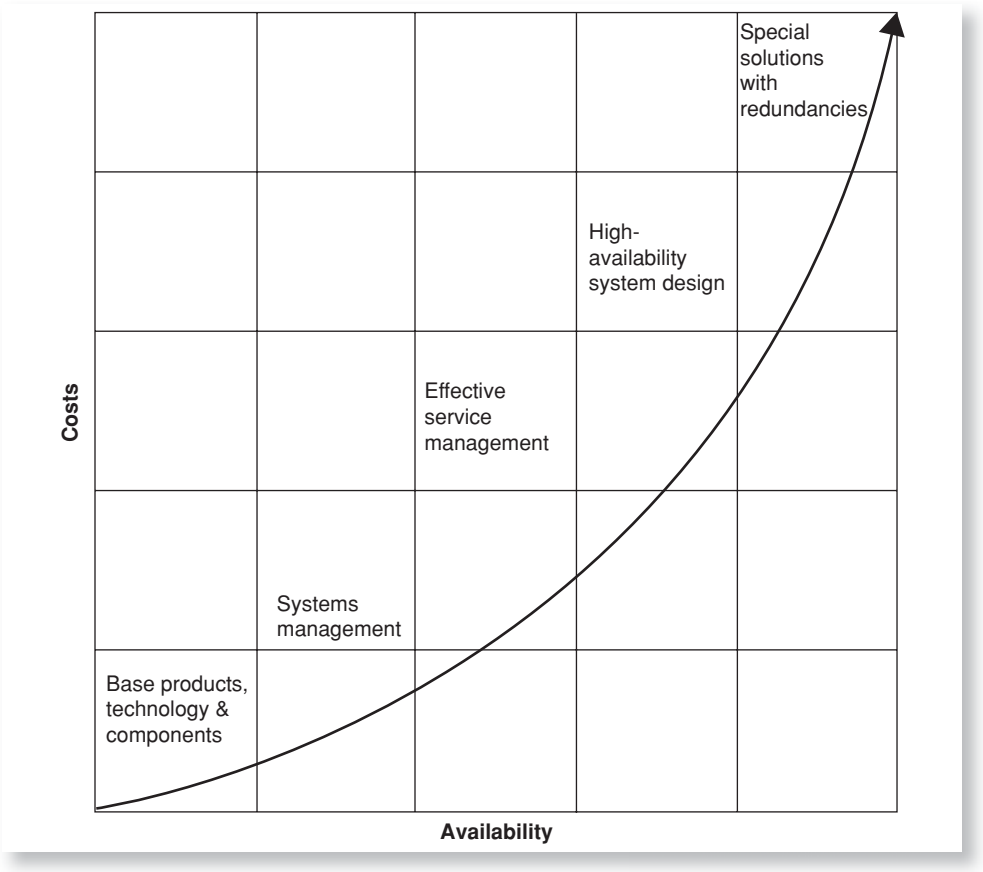

EXHIBIT 6.4 ITIL Availability and Costs Relationship

The main benefit of availability management is to have a structured process in place to deliver IT services that are provided according to the agreed requirements of the customers. This should result in a higher availability of the IT services and increased customer satisfaction. This covers an area where IT auditors can ask some hard questions as part of their IT general controls reviews.

Service Delivery Information Systems Security and Continuity Management

Security and continuity management represent two separate ITIL service delivery best practice components. As businesses are ever-more dependent on IT, the impact of any unavailability of IT services has drastically increased. Every time the availability or performance of a service is reduced, IT customers cannot continue with their normal work. This trend toward a high dependency on IT support and services will continue and increasingly influence direct customers, managers, and decision makers. ITIL continuity management emphasizes that the impact of a total or even partial loss of the IT

services should be estimated and continuity plans established to ensure that the business, and its supporting IT infrastructure, will always be able to continue.

ITIL calls for an appropriate strategy to be developed that contains an optimal balance of risk reduction and recovery options. These are some of the same business continuity and disaster recovery strategies as discussed in Chapter 10. Using the approaches outlined there, an IT organization should implement an effective set of service continuity processes.

IT security management is another set of ITIL best practices. ITIL recognizes the need for information security within the corporate governance framework to provide a strategic direction for security activities and ensures that these activities are achieved. Very much following an IT governance focus, ITIL emphasizes that security is more than just an IT issue; it's a management issue as well. The objectives of IT security are to protect the interests of those relying on IT information and the systems and communications that deliver it. ITIL information security is met through the following goals:

- **Availability objective.** Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures.
- **Confidentiality objective.** Information is observed or disclosed only to those who have a right to know.
- **Integrity objective.** Information is complete, accurate, and protected against unauthorized modification.
- **Authenticity and nonrepudiation objective.** Business transactions as well as information exchanges between enterprises, or with partners, can be trusted.

ITIL information security management goes on to outline best practices for a complete information security management system. A very important best practice, effective information security management processes are an important element of effective IT governance.

ITIL SERVICE TRANSITION MANAGEMENT PROCESSES

As IT managers and professionals recognize, IT operations have almost always been subject to regular hardware or software changes. These may involve proper transition planning to introduce the new components, testing and validation before any release to production, and configuration management to control the inventory and relationships of the IT equipment and services. ITIL has grouped these best practices into what it calls transition management, an area that can present some significant internal control risks for IT infrastructure operations. An IT application, for example, may be installed with solid internal controls. However, subsequent unauthorized changes to the same application or improperly configured attached equipment may introduce new control concerns.

Service Transition Change Management

The problem management process, discussed as part of service operations, often results in the need for IT changes such as program changes or process revisions to improve services or reduce costs. The goal of ITIL change management is to utilize standardized methods and procedures for the efficient and prompt handling of all changes, in order to minimize their impact on service quality and the day-to-day operations. ITIL change management processes include:

- IT hardware and system software.
- Communications equipment and software.
- All applications software.
- All documentation and procedures associated with the running, support, and maintenance of live systems.

The last point is of particular concern, since all too often IT hardware and software are changed with little concern given to changing the supporting documentation and related software. Changes to any IT components (e.g., applications software, documentation, or procedures) should be subject to a formal change management process. All too often, however, the change management process is haphazard at best. Examples here are changes to applications without thinking through their implications for the overall IT infrastructure, incident management fixes that create other changes, or senior management requests for changes to solve short-term or immediate problems. A formal change management process that reviews and approves any proposed changes will almost always improve IT and enterprise internal control processes. The ITIL change management process should be tightly linked to configuration management, discussed previously, to ensure that information regarding the possible implications of a proposed change is made available, and that any possible impacts are detected and presented appropriately.

Change management processes should have high visibility and open channels of communication in order to promote smooth transitions when changes take place. To improve this process, many IT functions have instituted a formal change advisory board (CAB), made up of people from both IT and other user functions within the enterprise, to review and approve changes. A CAB is a body that exists to approve changes and to assist in the assessment and prioritization of changes. It should be given the responsibility of ensuring that all changes are adequately assessed from both a business and a technical perspective. To achieve this mix, the CAB should consist of a team with a clear understanding of the customer business needs as well as the technical development and support functions. Chaired by a responsible change manager, the CAB should comprise IT customers, applications developers, various experts/technical consultants as appropriate, and any contractor or third parties' representatives if in an outsourcing situation. Although a CAB should meet regularly to review and schedule proposed changes, it should not act as an impediment to IT operations but should exist to provide an orderly scheduling and introduction of all types of IT infrastructure changes.

Efficient overall service management processes require a capability to change things in an orderly way, without making errors and taking wrong decisions. An

effective change management process is indispensable for an effective IT infrastructure and should include:

- Better alignment of IT services to business requirements.
- Increased visibility and communication of changes to both business and service support staff.
- Improved risk assessments.
- A reduced adverse impact of changes on the quality of services.
- Better assessments of the cost of proposed changes before they are incurred.
- Increased productivity of IT customers through fewer disruption delays and higher-quality services.
- A greater ability of IT to absorb a large volume of changes.

The ITIL change management process is an important component of IT infrastructure controls and should align tightly with the configuration, capacity, and release management key processes in the IT infrastructure. It is also important for effective IT governance.

Service Transition Configuration Management

Whatever their relative size, IT operations functions are complex, with multiple types and versions of hardware and software components as well as linkages to cloud computing components that all must work together in an orderly, well-managed manner. This is certainly true both for a major corporation with classic mainframe systems, "farms" of servers, and a multitude of storage devices and communications gear as well as for a small IT systems operation. A formal configuration management function is an important service delivery process that supports the identification, recording, and reporting of IT components, their versions, constituent components, and relationships. Items that should be under the control of configuration management include hardware, software, and associated documentation. Configuration management is not the same concept as the depreciation accounting process for asset management, although the two are related. Asset management systems maintain details on IT gear above a certain value, their business unit, and location. Configuration management also maintains relationships between assets, which asset management usually does not. Some enterprises start with asset management and then move on to configuration management.

A basic and important configuration management IT governance activity is to identify the various individual components in IT operations, called configuration items (CIs), and then to identify key supporting data for these CIs, including their "owners," identifying data, and version numbers, as well as systems interrelationships. This data should be captured, organized, and recorded in what is often known as a configuration management database (CMDB). The team responsible for configuration management should select and identify these configuration structures for the entire infrastructure's CIs, including establishing relationships between each CI and connected components in the overall IT infrastructure configuration. Going beyond just data entry on the CMDB, the process should ensure that only authorized CIs have been accepted and that no CI

is added, modified, replaced, or removed without an appropriate change request and an updated specification.

We should think of the importance of the configuration management process in terms of the IT applications in the typical business department. Every professional staff member probably has a smartphone or a laptop computer, but unless each has consistent versions of software, there may be difficulties in these systems communicating with one another. This is where configuration management is important. It is really more important when attempting to have an understanding of the various versions or even types of software and equipment in a large IT operation.

The configuration management process includes control elements important for effective overall IT governance. The IT team responsible for the configuration management process should maintain records for CI status and track the status of a CI as it changes from one state to another, for instance, from under development to being tested, going live, and then eventually being withdrawn. The CMDB is the repository for these CIs, but that database does not have to be a complex, specialized application. For example, an enterprise can establish a very basic CMDB by just using spreadsheets or local database systems. In today's large and complex IT infrastructures, however, configuration management often requires the use of physical and electronic libraries along with a CMDB to hold definitive copies of all software and supporting documentation. The CMDB should be based on a database technology that provides flexible and powerful interrogation facilities and defines the relationships between all system components.

The configuration management process interfaces directly with systems development, testing, change, and release management processes to incorporate new and updated product deliverables. In addition, the CMDB can be used by the service level management process to hold details of services and to relate them to underlying IT components. The CMDB can also be used to store inventory details of CIs, such as the supplier, cost, purchase date, and renewal date for a license. An additional bonus is the use of the CMDB to cover the legal aspects associated with the maintenance of licenses and contracts.

ITIL SERVICE OPERATION PROCESSES

The ITIL best practices described in this chapter started with the importance of setting service strategies, including basic IT policies and such higher-level areas as IT financial management. In the natural process of launching IT resources, the next set of best practices covers service design, processes that handle IT capacity and availability, as well as service level management to agree with users of IT services as to the services that will be provided. The last of these three linked ITIL processes is known as service operations, a process that allows the business customer to see the quality of the IT services offered.

Service operations cover the day-to-day service value that should be provided by IT systems and processes. The purpose of the ITIL service operation process is to help coordinate and deliver IT services to customers. This was a value concept that was often missing in the earlier days of IT operations, but ITIL best practices bring these concepts closer to business and management needs.

ITIL service operations define separate service operation processes for event and incident management, where events are defined as any detectable occurrence that has significance for the management of the IT infrastructure or delivery of related IT services. Although ITIL defines many similarities between what are called ITIL events and incidents, our discussion here will focus on incident management. The effective implementation of these processes will enhance overall IT governance operations.

Service Operation Event and Incident Management

Incident management processes cover the activities necessary for restoring an IT service following a disruption. ITIL defines a disruption as any type of problem that prevents an IT user from receiving expected adequate services, whether an overall system failure, the user's inability to access an application for any of a wide variety of reasons, a password failure due to a "fat fingers" typing error, or any other problem. The reported problem is called an *incident*, some type of deviation from standard operations. Although many IT operations have a function called a help desk or a customer support group, this general function is referred to here as the *service desk.* The service desk is usually the owner of the incident management process, although all service support groups across IT may have a role.

The objective of effective incident management processes is to restore normal operations as quickly as possible in a cost-effective manner with minimal impact on either the overall business or the user. What is meant by "quickly" should not be subject to interpretation, and ITIL calls for restoration time frame standards to be defined in service level agreements discussed in Chapter 17. Effective SLAs are an important component of the IT infrastructure, and their existence is important for IT governance practices. The first component of the ITIL incident management process is the detection and documentation of the incident by the service desk, as a single point of contact. These incidents can include such matters as a user calling in some specific application problem or IT operations informing the service desk of an application processing problem.

Once an incident is received, the service desk should classify it in terms of its priority, impact, and urgency. The definition of a reported incident's priority is one of the more important aspects of managing IT incidents. Every person who calls in an incident generally thinks that theirs is the most important, and the incident management function has the difficult task of defining the relative priority of the reported incident, its importance, and its impact on the business. Exhibit 6.5 outlines the life cycle of an IT incident from the initial call through resolution and closure. The point here is to understand service desk recommended best practices and to look for formal SLAs, as part of the service level management process, to define the priority with which incidents need to be resolved, the effort put into their resolution, and the recovery from incidents. These SLAs should depend on the *impact or criticality* of the incident for the reporting entity or overall enterprise. Incident management should assess, for example, how many users will suffer as a result of a reported technical failure of a hardware component. Similarly, a call regarding a problem with the month-end accounting close process should be assigned a higher level of criticality than a problem with an application that generates purchase orders.

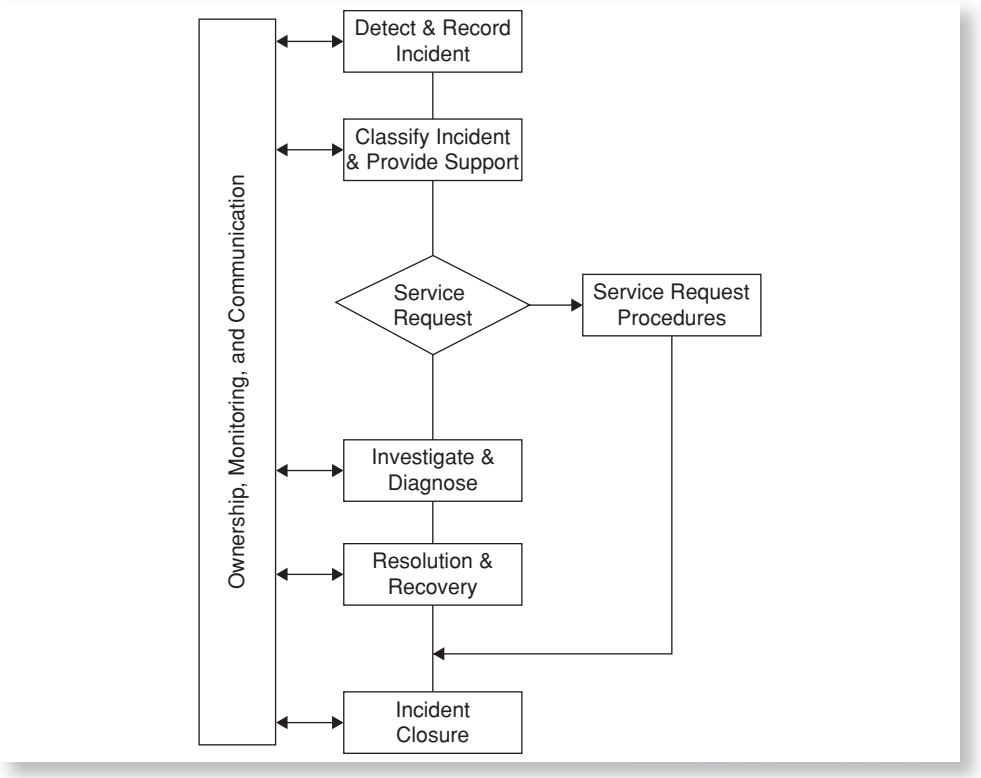

EXHIBIT 6.5 ITIL Incident Management Life Cycle

In addition, attention should be given to the *urgency* of the reported incident. Urgency refers to the speed necessary to solve an incident of a certain impact. A high-impact incident does not, by default, always have to be solved immediately. An incident call reporting that some user group cannot work at all because of some service outage is often of greater urgency than a senior manager calling to request a functionality change. The incident management team should investigate the reported incident as soon as possible to determine its extent. A reported failure of some component may just mean that a device is out of service or might indicate a server is down. Those types of incidents are often not very complex and can be repaired relatively easily. A telecommunications failure that might impact multiple international units and thus might delay the monthly financial close can be much larger in size and scope.

Once an incident has been logged in, the process of investigation and diagnosis should begin. If the service desk cannot solve the incident, it should be assigned to other IT support levels for resolution. However, all parties that work on the incident should keep records of their actions by updating a common incident log file. Some incidents can be resolved through a quick fix by the service desk, others by a more formal problem resolution, or in the case of more significant problems, by a workaround to get things back in partial operation coupled with a formal request for change (RFC) to systems, to a vendor, or whatever parties are needed to correct such a more significant problem. In

any event, efforts should be marshaled to correct the problem with the incident management function retaining ownership of the matter until resolution. Solid documentation should be maintained to track the incident until its resolution. The incident can be formally closed once matters have been fixed, or if not easily solved, the incident should be passed to the problem management process function as discussed next.

All ITIL processes are somewhat related to one another, but in many circumstances incident management represents the first line between users or customers of IT services and IT itself. Properly organized, incident management should be much more than the "help desks" of an earlier time when users called in with problems but frequently did not get much actual help beyond perhaps password resets. Incident management is a first point of contact between the customers—users—and the overall IT function. Incidents, the result of failures or errors within the IT infrastructure, result in actual or potential variations from the planned operation of services. Sometimes the cause of these incidents may be apparent and can be addressed or fixed without the need for further investigation. In other situations, there may be a need for a hardware or software repair, a matter that often takes some time to implement. Short-run solutions may be a workaround, a quick fix to get back in operation, or a formal RFC to the change management process to remove the error. An example of a short-term workaround might be simply instructing a customer to reboot a personal computer or resetting a communications line, without directly addressing the underlying cause of the incident.

Where the underlying cause of the incident is not identifiable, it is often appropriate to raise a problem record for the unknown error within the infrastructure. Normally a problem record is raised only if investigation is warranted, and its actual and potential impact should be assessed. Successful processing of a problem record will result in the identification of the underlying error, and the record can then be converted into a known error once a workaround has been developed, and/or an RFC.

Service Operation Problem Management

When the incident management process encounters a deviation with an unknown cause or reason, that incident should be passed on to the ITIL problem management process for resolution. The objective is to minimize the total impact of problems through a formal process of detection and repair as well as taking actions to prevent any reoccurrence. The problem management process is the next step in the criticality of some reported incident and should be considered in terms of three subprocesses: problem control, error control, and proactive problem management. ITIL defines a "problem" as an unknown underlying cause resulting from one or more incidents, and a "known error" as a problem that has been successfully diagnosed and for which a workaround has been identified. The idea is not necessarily to create a second administrative function in an IT enterprise to take reported help desk incidents, but to identify when and how some help desk reported incidents should be passed on to another person or authority to better diagnose the reported matter and treat it as a problem. An effective problem management process can do much to improve overall IT customer service.

In addition to solving any single incident that was *bumped up* to the problem management process, IT should try to establish processes for better problem and error control, including maintaining data to help identify trends and suggesting improved procedures for the proactive prevention of problems. Data should be maintained on solutions and/or any available workarounds for a resolved problem, as well as closed problem records. In many instances, problem management may encounter a situation where it is necessary to go a step further and file a formal RFC, either through an IT development function or through a hardware or software vendor.

The problem management process focuses on finding patterns between incidents, problems, and known errors. A detailed review of these patterns allows an analyst to solve the problem by considering the many possibilities and narrowing things down to a solution, what is called "root cause" analysis. There are many good techniques for resolving and correcting problems, often caused by a combination of technical and nontechnical factors. Problem management is a good area for diagnosing IT service delivery processes in order to better understand the overall health of IT operations. More information can be gathered through an understanding of the number of RFCs raised and the impact of those RFCs on the availability and reliability of the overall IT services covered, the amount of time worked on investigations and diagnoses for various types of problems by organization unit or vendor, the number and impact of incidents occurring before a root problem is solved or a known error is confirmed, and the plans for the resolution of open problems with regard to people and other resource requirements as well as related costs and budgeted amounts.

The ITIL service operation problem management processes are important for understanding and assessing the overall health of IT infrastructure operations. An efficient incident management process is necessary to receive customer calls and take immediate corrective actions, but an effective problem management process will go a step further to analyze and solve the problem, initiating RFCs where necessary and otherwise improving IT customer satisfaction.

IT GOVERNANCE AND ITIL SERVICE DELIVERY BEST PRACTICES

The preceding paragraphs have outlined some of the more critical ITIL service management life-cycle processes. ITIL service management outlines processes for launching, managing, and controlling all levels of IT services with an emphasis on establishing customer satisfaction. ITIL guidance goes beyond just internal controls and includes managing IT costs, establishing measurements and metrics, and other quality improvement measures.

ITIL calls for any IT function to build a program of continual service improvements to review, analyze, and make recommendations on improvement opportunities in each of the ITIL service delivery life-cycle phases discussed in these sections. ITIL service management life-cycle processes are increasingly being adopted by IT functions worldwide. The emphasis on service raises the importance of IT resources and its supporting infrastructure to the overall enterprise and its customers and stakeholders.

The ITIL service management life cycle is a series of interrelated best practice processes that support the management of the IT infrastructure and management of the enterprise. IT applications are in the center of this puzzle and are a key central area of internal controls and IT governance concerns. While the ITIL problem, incident, and change management processes, among others, tend to call for a very large IT function with multiple levels of staff and management resources, these ITIL best practices can also apply to a much smaller enterprise. ITIL applies to all sizes of IT functions! In order to be ITIL-compliant, an enterprise does not need multiple levels of support staff. Rather, it needs to think of the various service support and service delivery processes from an ITIL best practices perspective. A smaller IT function may not need to establish separate incident management and problem management functions, for example, but must think of each as separate processes with unique control procedures. Even if an enterprise IT function is very small, each ITIL process area should be treated as a separate area for process improvement.

The IT infrastructure is an important IT governance area of concern. All too often IT and other senior managers have concentrated their attention on the applications controls and the IT general controls of the past. In today's world of complex processes supporting the IT infrastructure, the ITIL processes outlined in this chapter describe some excellent areas for IT governance attention.

NOTE

1. ITIL publications are available from the UK agency called the Stationery Office (TSO), which can be found at www.tsoshop.co.uk.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER SEVEN

7

IT Governance Standards: ISO 9001, 27002, and 38500

IN THE YEARS FOLLOWING WORLD WAR II, the United States emerged as the worldwide economic and political leader. Due to this dominance, many in the United States all but ignored the commercial best practice standards developed and used elsewhere in our globally connected economy. These international best practice standards are collaborative efforts that take into account a wide range of national needs and requirements. The source of many of these standards is the International Organization for Standardization (ISO; www.iso.org), a body based in Geneva, Switzerland, that has issued well-recognized standards covering a wide range of areas from specifications for fastener screw threads in an automobile engine to the thickness of a personal credit card to IT quality standards. These standards have been expanded over the years to cover many areas that are important for enterprise governance and quality.

Senior executives should have an understanding of the role of any ISO standards that are appropriate in their enterprise as well as the standards that are important for effective IT governance. This chapter will review three of these standards that are important for effective IT governance practices. After a background discussion of how these ISO standards are developed and why they are important, we will first look at the international standard called ISO 9001. While not focused on IT governance issues specifically, the principles outlined in this standard have encouraged many enterprises on a worldwide basis to build and continually implement quality practices in their manufacturing and other business processes.

Although there are a wide range of ISO standards that may be applicable to IT governance, this chapter will review and describe the importance of two of them, ISO 27002 and ISO 38500. Related to our discussion in Chapter 17 on service level agreements, these standards outline a top-down framework to define the features of service management processes that are essential for the delivery of high-quality services.

An understanding of appropriate ISO standards can be important for some IT governance practices. While these standards are often implemented through an enterprise quality management or related enterprise function, a senior manager should have a general understanding of their importance and the overall ISO process.

ISO STANDARDS BACKGROUND

Confusing for some, ISO refers to the International Organization for Standards, a Geneva, Switzerland–based worldwide standards-setting authority. The ISO is responsible for developing and publishing a wide range of international standards in many business and process areas. Some of these standards are very broad, such as ISO 14001, outlining requirements for effective environmental control systems, while others are detailed and precise, such as a standard covering the size and thickness of a plastic credit card. The broad ISO standards are important because they allow all worldwide enterprises to be talking in the same language when they can claim that they have, for example, an effective ISO 14001 environmental control system. Many of the more detailed standards are also very critical, such as those for an automated teller machine anywhere in the world to expect to receive the same size and thickness of credit card.

ISO standards are developed through the collaborative efforts of many national standards-setting organizations, such as the American National Standards Institute or other groups throughout the world. The standards-setting process begins with a generally recognized need for a standard in some area. An example would be ISO 27001, which outlines the high-level requirements for an effective information security management system. This standard was developed through the efforts of international technical committees sponsored by the ISO in cooperation with the International Electrotechnical Commission, an international standards-setting group. The standard is not specific in its detailed requirements but contains many high-level statements along the lines of "The organization shall." In some respects, this type of guidance is built into IT audit procedures discussed in many of these chapters.

Because of the numerous international governmental authorities, professional groups, and individual experts involved in the ISO standards-setting process, the building and approval of any ISO document typically is long and slow. An expert committee develops an initial draft standard covering some area; the draft then is sent out for review and comments with a review response due date; and the ISO committee finally reviews draft comments before either issuing the new standard or sending a revised draft out for yet another round of reviews and suggested changes. Typically after many drafts and comment periods, the ISO standard is published. Enterprises can then take the necessary steps to comply with the standard. To certify their compliance, they must contract with a certified outside auditor, with skills in that standard, to attest to their compliance.

Many U.S. enterprises first got involved with these international standards through the 1980s launch of ISO 9000 quality management system standards discussed later in this chapter. U.S. companies had trouble competing against products with the high-quality design standards found in many non-U.S. products at that time, such as Japanese automobiles. Japanese enterprises had designed many high-quality products by

following what became ISO 9000, and U.S. manufacturers began to modify their own processes to comply with these higher standards of product quality. Compliance with the ISO 9000 standard allowed worldwide enterprises to design their operations in accordance with a single, consistent standard and then to assert that they have a quality management system in place in accordance with the international standard.

ISO standards are much more specific and controlled than the Information Technology Infrastructure Library (ITIL) best practices guidelines discussed in Chapter 6. The standards are published and controlled by the ISO organization in Geneva, following strict copyright rules. The materials cannot be downloaded through a casual Web search; they must be purchased. Many of the actual ISO standards are very detailed outlines of practices to be followed.

The guidance is clear and unambiguous and often points to other sections of this standard for follow-up. An enterprise can follow and rely on ISO standards similar to the ITIL best practices, but ISO standards are much more than ITIL's recommended best practices. They represent performance measures for an enterprise and its peers. By adhering to these worldwide standards, an enterprise can verify that it is operating in accordance with a consistent international standard. ISO 13485 on quality management regulatory requirements for medical devices provides an example. This standard defines the quality requirements covering human health care devices, and among other matters, the standard calls for an enterprise manufacturing such devices to establish appropriate calibration controls. Because of the diversity of calibration approaches, the standard cannot specify just one approach; it does, however, require that enterprises have appropriate mechanisms in place.

It is one thing for an enterprise to read an ISO standard and change its processes to follow it; it is another thing to demonstrate to others that it is following the standard. This ISO certification is a process similar to an external audit of financial records performed by certified public accountants (CPAs). Financial statement audits require a licensed CPA external auditor to assess whether an enterprise's financial reports are "fairly stated," following good internal controls and recognized accounting standards. These are high-level words, but such a signed external audit report along with the final reported results provides a level of assurance that the financial reports are fairly stated and are based on good internal control procedures.

The ISO certification process is also similar to a CPA-led financial audit that is based on compliance with generally accepted auditing standards (GAAS) performed by major public accounting firms. While no "Big 4" set of major ISO auditing firms exists, national standards-setting organizations qualify outside reviewers to perform external audits of various ISO standards. There is no ISO GAAS, but a wide degree of diversity in audit objectives, since a reviewer for ISO 27001 on IT security management systems will be looking for different control procedures than would an ISO auditor for 13485 medical device quality management systems. In all cases, however, the qualified ISO outside auditor may identify areas for corrective actions and publish a report to management similar to internal audit processes, as discussed in Chapter 19. Once the ISO auditor's recommendations are corrected, the outside reviewer will certify that the enterprise is in compliance with the standard.

Once certified, the enterprise can advertise to the outside world that it has a process in place that meets that specific ISO standard. For example, a customer for the

medical diagnostic device would want to know if a potential supplier is in compliance with ISO 13485. That same medical device manufacturer would also want to gain assurance that its prime component suppliers are ISO qualified. Although there are a wide range of ISO standards, the next sections discuss several that are important in today's world of heightened internal controls and governance.

ISO 9000 QUALITY MANAGEMENT STANDARDS

ISO 9000 has a heritage dating back to World War II, when both sides of the conflict required strong product uniformity while operating at extremely high levels of production volume. Even if the products produced were bullets and bombs, they still had to work correctly, and there was a need for strict product quality control. On the Western Allies' side there arose some strong quality assurance standard procedures, as well as the professions of industrial engineer and production quality control specialist. After the war, ISO was established as part of the General Agreement on Trade and Tariffs, one of the international agreements to bring the world to a more peaceful environment. ISO 9000 on quality management systems was one of the earlier ISO standards. It first received most attention in the newly recovering European countries.

Japan was another rebuilding and recovering postwar country that strongly embraced quality management systems. In the 1950s and 1960s, the Japanese invited a series of U.S.-based quality systems experts, such as W. Edwards Deming[1] and others, to help at many of their plants. While these quality systems experts had been all but ignored in the United States, their philosophies and techniques were heavily embraced by Japanese industry, and by the mid-1970s Japanese electronics and automobile manufacturers began to make deep inroads into U.S. markets due to the quality and value of their products. Many in the United States began to recognize that these Japanese-manufactured products were superior in many respects to their own. ISO 9000 quality standards became an increasingly important factor to measure and assess the quality of products worldwide.

ISO 9000 is a family of standards for quality management systems. Maintained by ISO, these include requirements for such matters as:

- Monitoring processes to ensure that they are effective.
- Keeping adequate business process records.
- Checking production outputs for defects, with appropriate corrective actions initiated where necessary.
- Regularly reviewing individual processes and the overall quality system for effectiveness.
- Facilitating continual improvement processes.

Each of these items refers to processes, not specific actions. For an enterprise to assert that it is in compliance with ISO 9000 (actually 9001), for example—that it is monitoring key processes to be effective—often it must make significant changes to its management procedures and supporting documentation. Compliance with an ISO standard also creates a required level of expectation. Any enterprise, on a worldwide

scope, that holds to such standards is stating that it has effective quality systems in place. An enterprise that has been independently audited and certified to be in conformance with ISO 9001, for example, may publicly state that it is "ISO 9001 certified" or "ISO 9001 registered." Certification to an ISO 9000 standard does not guarantee the compliance (and therefore the quality) of end products and services; rather, it certifies that consistent business and production processes are being applied.

The actual certification is achieved through a review by a registered ISO auditor certified for the particular ISO standard. As discussed, this process is similar to the CPA's review and certified audit of an enterprise's financial statements. Regulated by their national standards organizations, ISO auditors are authorized to register an enterprise's compliance with unique ISO standards.

ISO 9000 and other ISO standards impose heavy documentation requirements on an enterprise. It is not sufficient for an enterprise just to claim that some process has been once documented. There must be an ongoing process to keep that documentation current over time. In past years, many enterprises went through onetime efforts to create documentation for some new initiative but failed to keep it current. Many IT auditors have faced this kind of situation. Auditors frequently ask if some system or process they are reviewing is documented, but if the documentation is out of date or nonexistent, this shortcoming often would become an audit report finding but too often would result in little definitive corrective action. ISO 9000 compliance raises documentation requirements for quality processes to a whole new level. An ISO reviewer must certify that the enterprise is in compliance in order for the enterprise to advertise to the outside world that it is in compliance with the ISO standard.

ISO 9000 is a set of standards for a continual improvement–driven quality system, be it for a manufactured component or a service process. Exhibit 7.1 shows such a quality management system process that is driven by internal procedures for continual improvements as well as customer requests. In this continual process, existing processes should be monitored, actions planned for improvements, and the action items implemented for subsequent monitoring and further improvements. For many senior managers, the continual improvement quality process is nothing new. IT systems development professionals have used essentially the same set of general processes since the early days of IT systems development, in a process to develop new IT systems called the systems development life cycle (SDLC). Many of these SDLC-developed applications called for a great deal of documentation, which often was not prepared. Today's IT applications are developed through more informal and iterative rapid application development processes.

Solid and accurate documentation is extremely important for an enterprise seeking to claim ISO registration, a global requirement. ISO best practices call for a hierarchy of documentation in any area, starting with top-level manuals to explain the *why*s and then down to instructions describing the *how*s of the practice. Exhibit 7.2 shows this documentation hierarchy with "Documentation & Forms" on the bottom part of the triangle, providing proof. This documentation is essential to support a quality management system and certainly is required by ISO external certification auditors.

This section has provided a very high-level description of the ISO 9000 quality management process. However, the reader may ask, "Why should I care about ISO, and what does it have to do with IT governance?" Compliance with these ISO 9000 processes

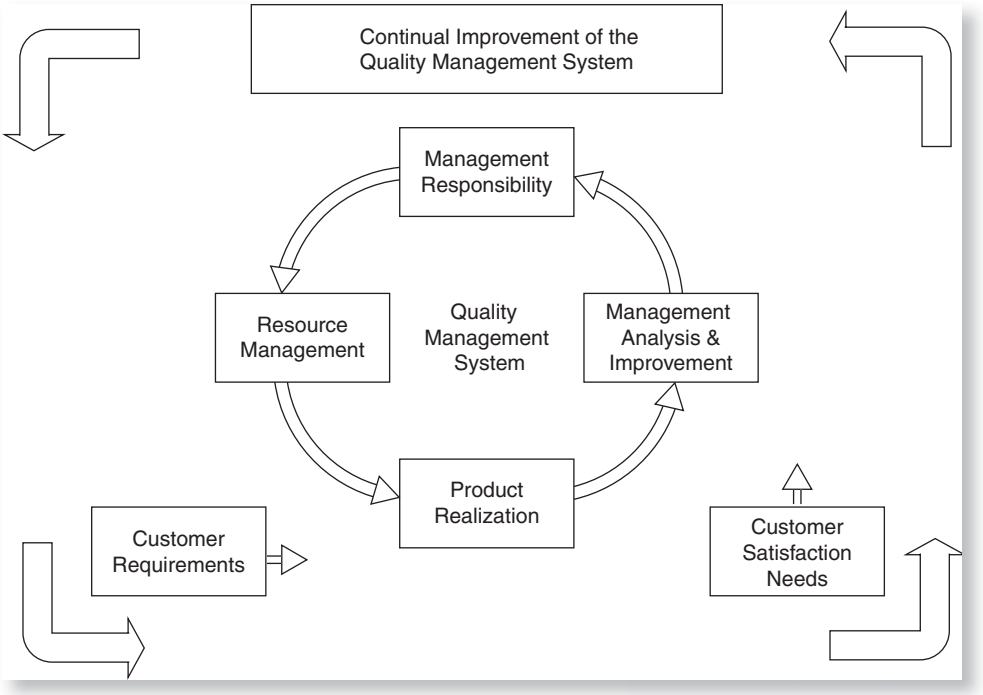

EXHIBIT 7.1 Quality Management System Process

is important for all types of enterprises to attest to their own internal management and to the outside world that the enterprise is focused on quality. As an example, in 1995, the American Institute of Certified Public Accountants became the first major worldwide professional organization to become ISO 9001 certified.[2] Organizations of all levels should consider adopting ISO 9000 processes. An advertisement for many types of

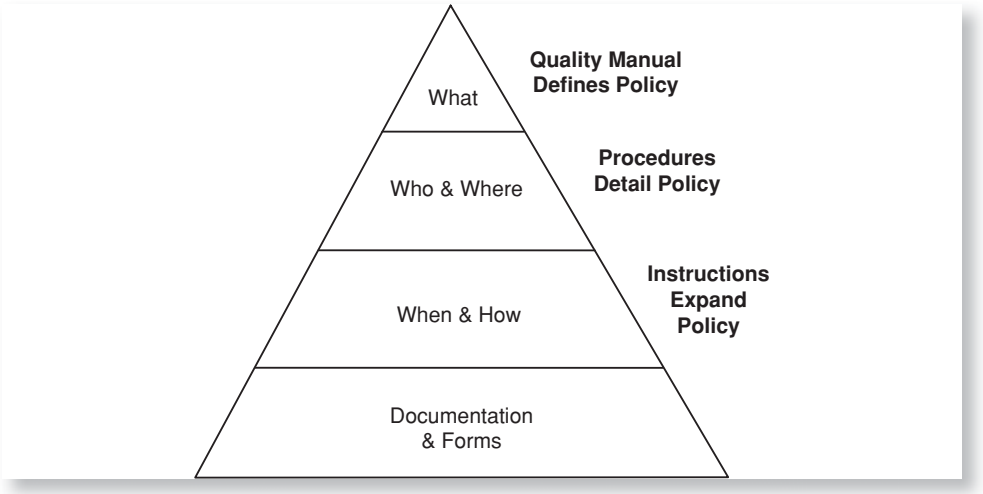

EXHIBIT 7.2 ISO Documentation Hierarchy

product or service offerings today will state that the vendor is ISO quality certified, and any customer can consider asking for more information about that level of certification before deciding to complete a purchase transaction.

ISO standards outline some high best practices in many areas of IT operations. Even if an enterprise does not go 100 percent in completing all of the requirements for a given ISO standard and completes ISO auditing requirements, the standards will provide some solid guidance for building strong internal processes. The sections following discuss, in more detail, the requirements for two of these standards that are important to effective IT governance processes.

ISO IT SECURITY STANDARDS: ISO 27002 AND 27001

ISO 27002 is an important IT-related security standard designed to help any enterprise that needs to establish a comprehensive information security management program or improve its current information security practices. Going beyond the topics of governance and IT security discussed in Chapter 10, ISO 27002 is a standard about both a wide range of information sources and information security in a general sense. Because such information can exist in many forms, the standard takes a very broad approach and includes a wide range of standards covering security regarding:

- Data and software electronic files
- All formats of paper documents, including printed materials, handwritten notes, and photographs
- Video and audio recordings
- Telephone conversations, as well as e-mail, fax, video, and other forms of messages

The idea here is that all forms of information have value and need to be protected, just like any other corporate asset. Many enterprises today do not even consider security standards in these broad areas, but the ISO standard suggests they should be covered when appropriate. In addition, the infrastructure that supports this information, including networks, systems, and functions, also must be protected from a wide range of threats, including everything from human error and equipment failure to theft, fraud, vandalism, sabotage, fire, flood, and even terrorism.

Similar to all other ISO standards, this published standard does not really prescribe *what* is specifically required but outlines areas where security-related standards are required. Exhibit 7.3 outlines major ISO 27002 topics. The standard does not contain detailed requirements for each of these areas—a thorough and consistent international standard would require a huge, extensive text that would not be all-inclusive and would soon be out of date. Rather, as an example, line 4.2 calls for security standards covering third-party access policies. ISO calls for the enterprise to have documented and approved processes covering third-party access policies. An enterprise should develop its own more detailed standards and procedures in this area. The type and extent of these standards can depend on many factors, but an ISO 27002-compliant enterprise should address this issue along with the other topic areas in the standard.

EXHIBIT 7.3 ISO 27002 Standards Topic Areas

This outline lists the high-level topic areas found in this ISO standard. The actual standard outline goes down to multiple and more detailed levels for each of the points. This level of detailed outline is typical of all ISO standards.

1. Scope: A high-level description of the application of this standard.
2. Terms and definitions: Consistent with other ISO standards, all major terms are defined (e.g., definition of what is meant by "Confidentiality")
3. The standards or need for a high-level information security policy
4. Requirements for an enterprise security organization:
   - 4.1 Information security infrastructure
   - 4.2 Security and third-party access policies
   - 4.3 Outsourcing considerations
5. Asset classification and control standards:
   - 5.1 Accountability for assets
   - 5.2 Information classifications
6. Personnel security:
   - 6.1 Security considerations in job definitions and resources
   - 6.2 User training for personnel security
   - 6.3 Standards for responding to security incidents and malfunctions
7. Physical and environmental security, including requirements for:
   - 7.1 Secure areas
   - 7.2 Equipment security
   - 7.3 General controls
8. Communications and operations management:
   - 8.1 Operational procedures and responsibility
   - 8.2 System planning and acceptance
   - 8.3 Protections against malicious software
   - 8.4 Housekeeping
   - 8.5 Network management requirements
   - 8.6 Media handling and security
   - 8.7 Exchanges of information and software
9. Access control:
   - 9.1 Business requirements for access control
   - 9.2 User access management
   - 9.3 User responsibilities for security standards
   - 9.4 Network access control
   - 9.5 Operating system access control
   - 9.6 Application access management
   - 9.7 Monitoring standards for systems access and use
   - 9.8 Mobile computing and related networking
10. System development and maintenance standards:
    - 10.1 Security requirements hardware and software systems
    - 10.2 Application systems security
    - 10.3 Cryptographic controls

EXHIBIT 7.3 (*Continued*)

10.4 Security of system files
10.5 Security in development and support processes

11. Business continuity management standards

12. Security standards covering compliance issues:

12.1 Compliance with legal requirements
12.2 Reviews of security policy and technical compliance
12.3 Systems audit considerations

As a first step to implementing ISO 27002, an enterprise should identify its own information security needs and requirements. Doing this requires performing an information security risk assessment along the lines of the Committee of Sponsoring Organizations (COSO) enterprise risk management processes discussed in Chapter 4. Such an assessment should focus on the identification of major security threats and vulnerabilities as well as an assessment of how likely it is that each will cause a security incident. This process should help to pinpoint an enterprise's unique information security needs and requirements.

To establish ISO 27002 information security standards-setting processes, an enterprise should identify and understand all of the legal, statutory, regulatory, and contractual requirements that it and its trading partners, contractors, and service providers must meet. Doing this requires an understanding and identification of an enterprise's unique legal information security needs and requirements.

ISO 27002 is the first of a series of international standards meant for any enterprise that uses internal or external computer systems, possesses confidential data, depends on IT to carry out its business activities, or simply wishes to adopt a higher level of security by complying with a standard. Just as ISO 9000 has become a guarantee of quality, compliance with the ISO 27002 standard enables partners to be confident in an enterprise's overall security. Compliance should promote an increased level of mutual confidence between partners, where each can attest that it has established security standards in compliance with a recognized set of standards. In addition, as ISO 27002 compliance becomes more common, it may result in lower premiums for computer risk insurance but certainly will yield better protection of confidential data and improved privacy practices and compliance with privacy laws. ISO 27002 is a structured and internationally recognized methodology that should help an enterprise to develop better management of information security on a continuing basis.

Supporting this high-level security controls standard, ISO 27001 is what the ISO defines as the "specification" for an IT security management system. That is, this standard is designed to measure, monitor, and control security management from a top-down perspective, and it explains how to apply ISO 27002 and defines the implementation of this IT security standard as a six-part process:

1. **Define a security policy.** A fundamental component of any standard is the need for a formal policy statement approved by senior management. All other compliance aspects of the standard will be measured against this policy statement.

2. **Define the scope of the IT security management system (ITSMS).** ISO 27002 defines security in rather broad terms that may not be appropriate or needed for all enterprises. Having defined a high-level security policy, an enterprise needs to define the scope of its active ITSMS. For example, ISO 27002 defines an element of security requirements as video and audio recordings. This may not be necessary for a given enterprise and then would be specifically excluded for its ITSMS scope.
3. **Undertake a risk assessment.** The enterprise should identify a risk assessment methodology that is suited to its ITSMS environment and then both develop criteria for accepting risks and define what constitutes acceptable levels of risk.
4. **Manage the risk.** This is a major process that includes formal risk identification, risk analysis, and options for the treatment of those risks. The latter can include applying appropriate risk avoidance controls, accepting risks, taking other steps to avoid them, or transferring the risks to other parties such as insurers or suppliers.
5. **Select control objectives and controls to be implemented.** This is very similar to the COSO internal controls procedures discussed in Chapter 4 as well as COBIT internal control processes discussed in Chapter 5. For each defined control objective, the enterprise should define an appropriate controls procedure.
6. **Prepare a statement of applicability.** This is the formal documentation that is necessary to wrap up the ITSMS documentation process. Such documentation matches up control objectives with procedures to manage and implement the ITSMS.

As can be seen from these six steps, risk analysis and security policies are fundamental to this ISO IT standard. Because of strict ISO copyright rules, we have not included specific extracts of ISO 27001 in this chapter. The actual ISO standards are presented in tight and unambiguous text. Little specific detail is provided, but there is enough to allow an enterprise to implement its ITSMS. Each formal standard concludes with an appendix section listing control procedures for each of the objective details in the standard. However, ISO 27001 should not be considered as a comprehensive set of control procedures that will change as technology changes; rather, it is an outline for the framework of an ITSMS that should be continually implemented, monitored, and maintained.

ISO 27002 and ISO 27001 are global standards, with established compliance and certification schemes in place, particularly in the United Kingdom and the European Union. Both standards will continue to evolve and to track technology and will expand with even wider changes. The standards provide a basis for defining effective IT security standards.

ISO 38500 IT GOVERNANCE STANDARD

ISO standards are developed and then issued in areas where there is a perceived need for best practices guidance on an international level. Sometimes these standards are released when there is a strong commercial need for product standardization. Our previously referenced ISO standard covering the size of consumer credit and debit payment cards is an example here. In the early days of credit cards, card providers issued them with different sizes, numbering schemes, and other factors. Standards of interchangeability

were needed to promote e-commerce, and an ISO standard was released. In some other cases, ISO standards represent best practices where compliance is necessary for commercial purposes. Our previous discussion on ISO 9000 quality standards is an example of this. Virtually every product manufacturing enterprise today that wants to compete on an international basis must be certified to be in compliance with ISO 9000 quality management system standards.

While some ISO standards have been in place for many years, ISO 38500 on IT governance is relatively new, having been released in 2008 after a long development period. It also has not received that great of a level of international attention at present, although the planned new versions of COBIT, discussed in Chapter 5, will incorporate ISO 38500 principles. In addition to the COSO internal control framework discussed in Chapter 4, COBIT in Chapter 5, and ITIL best practices in Chapter 6, ISO 38500 is another framework to help support effective IT governance practices for an enterprise. The standard to date has been released at a very high level, and more detailed sections and guidance are sure to follow. This section will provide a description of ISO 38500 and how it can help an enterprise establish effective IT governance practices.

ISO 38500 Objectives

This standard provides a framework of principles for senior managers to use when evaluating, directing, and monitoring the use of IT in their enterprise. This should assist senior managers to understand and fulfill their legal, regulatory, and ethical obligations in respect to their enterprises' use of IT. The framework comprises definitions, principles, and a governance model with the three objectives of:

1. Providing assurances to all enterprise stakeholders that they can have confidence in their organization's corporate governance of IT.
2. Informing and guiding senior managers in governing the use of IT in their organization.
3. Providing a basis for the objective evaluation of the corporate governance of IT.

ISO 38500 is also intended to guide those involved in designing and implementing senior management systems on effective policies and processes that support IT governance. That is, while its guidance refers to more senior-level management, all professionals involved with designing, implementing, managing, or reviewing an IT process should give some consideration to these broad standards.

This standard applies to the governance of IT management and decision processes that are controlled by IT specialists within the organization, by external service providers, or by other enterprise business units. The standard's objective is to provide guidance to IT professionals advising, informing, or assisting senior executives, including:

- Senior managers
- Members of groups monitoring the resources within the organization
- External business or technical specialists, such as legal or accounting
- Specialists, retail associations, or professional bodies

- Vendors of hardware, software, communications, and other IT products
- Internal and external service providers (including IT consultants)
- IT auditors

The listed objectives and scope are fairly broad and extensive for a relatively small and new standard. However, there are some major general principles buried in its current text, and we can expect to see much more detailed supporting definitions and guidance on ISO 38500 in future years.

The ISO 38500 Framework for IT Governance

The standard sets out six principles for good IT governance that are applicable to most enterprises. These principles express a preferred behavior to guide IT governance–related decision making. That is, a statement of each principle refers to what should happen, but it does not prescribe how, when, or by whom the principles would be implemented, as these aspects are dependent on the nature of the organization implementing the principles:

Principle 1: Responsibility. Individuals and groups within the enterprise should understand and accept their responsibilities in respect to both supply of and demand for IT services and resources. Those with responsibility for actions also have the authority to perform those actions.
Principle 2: Strategy. An enterprise's business strategy should take into account the current and future capabilities of IT; these strategic plans for IT should satisfy the current and ongoing needs of the enterprise's business strategy.
Principle 3: Acquisition. IT component or resource acquisitions should be made for valid reasons, on the basis of an appropriate and ongoing analysis, with clear and transparent decision making. There should be an appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.
Principle 4: Performance. IT should be fit for purposes of supporting the enterprise, providing the services, levels of service, and service quality required to meet current and future enterprise business requirements.
Principle 5: Conformance. IT should comply with all mandatory legislation and regulations, with policies and practices clearly defined, implemented, and enforced.
Principle 6: Human behavior. IT policies, practices, and decisions should demonstrate respect for human behavior, including the current and evolving needs of all the people in the process.

In addition to these basic principles, the standard provides a model for IT governance, as shown in Exhibit 7.4. The overall IT governance process is described in Exhibit 7.4 in the center triangle with business needs and business pressures requiring IT governance changes and actions. The model shows business pressures and business needs influencing the IT governance process. Governance processes then sit above overall IT processes where various proposals from IT influence IT governance processes. In addition, the IT governance process provides plans and policies to IT and the overall IT function provides performance and conformance information to IT governance. The basic overall process has been described in other chapters, but ISO 38500 does a good job in encapsulating this issue.

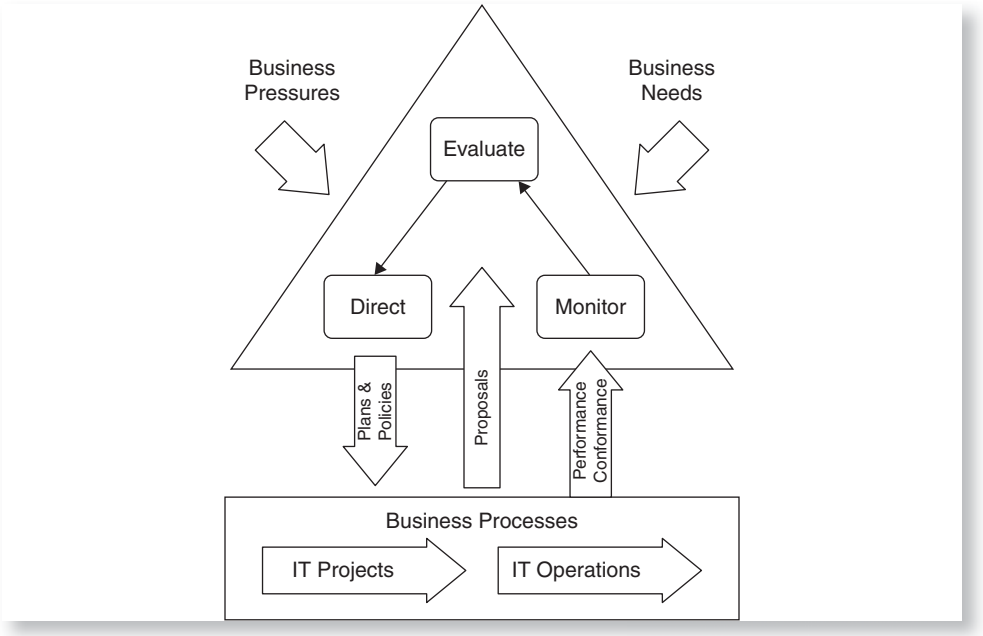

EXHIBIT 7.4 ISO 38500 Enterprise IT Governance Model

Inside the IT governance triangle in Exhibit 7.4, there are three process functions named evaluate, direct, and monitor. The ISO standard provides a definition for each of these:

1. **Evaluate.** IT senior managers should examine and make judgments on their current and future use of all IT resources, including strategies, proposals, and supply arrangements (whether internal, external, or both). In evaluating the use of IT, management should consider the external or internal pressures acting upon the business, such as technological change, economic or social trends, and political influences.

   Senior management should undertake these evaluations continually, as pressures change. They should also take account of both current and future business needs—the current and future organizational objectives that they must achieve, such as maintaining competitive advantage, as well as the specific objectives of the strategies and proposals they are evaluating.
2. **Direct.** Senior management should assign responsibility for and direct the preparation and implementation of plans and policies. Plans should set the direction for investments in IT projects and IT operations. These policies should establish sound behavior in the use of IT.

   Directors should ensure that the transition of projects to operational status is properly planned and managed, taking into account impacts on business and operational practices as well as existing IT systems and infrastructure.

   Senior IT management should encourage a culture of good IT governance by requiring managers to provide timely information, to comply with direction, and to conform with the six principles of good governance.

3. **Monitor.** Senior management should monitor, through appropriate measurement systems, the overall performance of IT. They should reassure themselves that this performance is in accordance with plans, particularly with regard to business objectives. Management should also make sure that IT conforms with regulatory, statutory, and contractual external obligations as well as with internal work practices.

Guidance for Implementing the ISO 38500 Standard

The ISO published standard then takes ISO 38500's six principles and folds them into the IT governance model to provide more specific IT governance guidance. This guidance as well as all details of the standard can be purchased in hard copy or downloaded from the ISO Web site (www.iso.org/iso/catalogue_detail?csnumber=51639). ISO copyright rules do not allow us to reproduce this published guidance, but we have edited and extracted a small portion of this guidance to provide some insights into the actual materials.

Using the strategy principle, for example, there is guidance for each of the evaluate, direct, and monitor action steps. Although modified from the actual standard and certainly not meant to represent the actual ISO 38500 standard, the following represents the guidance for the two standard principles:

- Principle 1, Strategy to Evaluate:
  - Senior management should evaluate developments in its IT and business processes to ensure that IT will provide support for future business needs.
  - In considering plans and policies, senior management should evaluate its IT activities to ensure that they align with the enterprise's objectives for changing circumstances, take consideration of better practices, and satisfy other key stakeholder requirements.
- Principle 2, Strategy to Monitor:
  - Senior management should monitor the progress of approved IT proposals to ensure that they are achieving objectives in required time frames using allocated resources.
  - Senior management should monitor the use of IT to ensure that it is achieving its intended benefits.

The standard continues with this general style of language. There are no specific rules or detailed procedures but just some general good guidance. But when a standard calls for senior management to "monitor the progress of approved IT proposals to ensure that they are achieving objectives in required time frames," this type of language points to the need for IT project and program approval processes, project planning with established time frames, and just regular senior management reviews. The enterprise's internal audit function, as discussed in Chapter 19, can act as an internal consultant and provide help in implementing this standards guidance, and Chapter 16, for example, talks about the importance of project management procedures.

There are many other applicable ISO standards, but ISO 38500 can help and strengthen overall enterprise IT governance. Many managers have rejected some of

these standards because they seem to require too much documentation or are too paperwork-intensive. That is, if a standard says that "management should monitor" some process or activity, the enterprise group supporting this area should be in a position to demonstrate this monitoring activity through some level of documentation. Of course, we are not talking about cabinets of paperwork, but some forms of retrievable electronic evidence. Many enterprises today that provide products or services in international markets have gone through the process of an ISO external audit to attest to their compliance with ISO 9000. In future years, we may see similar compliance requirements for ISO IT governance standards as they are expanded and become more recognized.

NOTES

1. William Edwards Deming (October 14, 1900–December 20, 1993) was an American statistician, professor, author, lecturer, and consultant. He is perhaps best known for his work in Japan but was a worldwide leader of the quality movement.
2. Norman Ho, "ISO 9000: No Longer a Stranger to Service," Gartner, www.qualitydigest.com/june99/html/body_iso_9000.html.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER EIGHT

IT Governance Issues: Risk Management, COSO ERM, and OCEG Guidance

RISK MANAGEMENT IS AN INSURANCE-RELATED CONCEPT where an individual or an enterprise will envision some type of threat, such as the danger of a residential fire or theft, and then will take actions to provide protections in the event that threat occurs. The most common risk protection approach is to purchase insurance from a commercial outside vendor or install protection mechanisms to provide some protection over the risks, using a risk-based approach to decide what type and how much insurance to purchase or what protection to install. Key decision factors here are the extent of perceived risks or other threats and the insurance and protective device costs to cover those risks.

Although individuals often think of risks and insurance protection in terms of the threat of fires, natural disasters, or theft, an enterprise needs to consider risks on a much broader level, which can include such things as the failure of a new business venture, malicious litigation because of a product failure, or unexpected economic bad turns. An enterprise cannot just easily buy insurance, in a cost-effective manner, to cover those other risks. Rather, an enterprise needs to implement other processes to provide protection from these many and varied business risks. An enterprise's IT resources are often a major area, where the physical destruction of their IT equipment, a disruption in network connections, or the theft of data resources is a significant risk to an enterprise that can have serious consequences unless there are adequate risk management and remediation tools installed and in place.

This chapter discusses risk management tools and techniques from the perspective of their importance for IT governance and also reviews some risk management fundamentals that should be important knowledge areas for all enterprise managers. This chapter then introduces COSO ERM, the specialized COSO enterprise risk management framework that is similar but has different objectives from the COSO internal control framework introduced in Chapter 4.

The chapter will conclude with an introduction of the Open Compliance and Ethics Group (OCEG) GRC model and an emphasis on its risk management standards. The OCEG is an industry standards group that has built and introduced a GRC capability model that has a strong emphasis on enterprise risk management. The OCEG has released a set of best practices GRC materials, but it does not have the same standards-setting importance as SOx rules or ISO standards, each discussed in earlier chapters. However, they soon may gain in their recognition and industry acceptance, and OCEG compliance can be important for IT governance.

RISK MANAGEMENT FUNDAMENTALS

Whether it be to select and purchase fire insurance for a new building facility, to install protective tools for a new business venture, or to purchase an appropriate level of what is known as directors and officers (D&O) liability insurance for the enterprise, senior management must realize that they are dealing with a variety of enterprise risks that must be understood and appropriately managed. Risk management should be thought of as a four-step process:

1. **Risk identification.** An enterprise needs to identify the issues and circumstances that can become significant risks to its operations.
2. **Quantitative or qualitative assessments of the documented risks.** Having identified potential risks, a next step is to employ tools to estimate the potential impacts if any of these identified risks occur.
3. **Risk prioritization and response planning.** The more significant identified risks should be prioritized, and response plans should be developed in the event of those risks occurring.
4. **Risk monitoring.** Ongoing processes should be installed to assess the current statuses of identified risks and both to take action if they occur and to assess the progress of those remedial actions.

This very general risk management process should be enterprise-wide, involving people at all levels and in all enterprise units. While a larger enterprise may want to organize a specialized team of risk management professionals, smaller enterprises also should designate people to be responsible for managing their enterprise-wide risk assessment process. Whether a formal risk management function or ad hoc risk management efforts, enterprise risk management should involve a wide range of people at various organization levels. A financial executive will have a different perspective on certain IT-related systems risks than would the chief information officer (CIO) or a member of the IT operations staff. Each sees and looks at risks from different perspectives. This same analogy is true for all aspects of the enterprise.

The previous four-step risk management process should be implemented at all levels of the enterprise and with the participation of many different people. Whether a smaller enterprise with a few facilities in a limited geographic area or a large, worldwide enterprise, common risk management approaches should be developed. This is particularly

important for the worldwide enterprises so common today. They may have multiple operating units engaged in different business operations and facilities in different countries. Some risks in one unit may directly impact or be related to risks in another, but other risk considerations may be effectively independent from the whole. These common risks can occur because of a wide variety of circumstances, ranging from poor financial decisions to changes in consumer tastes to new government regulations. Effective risk management processes are important elements of effective IT governance.

Risk Identification

While our emphasis is on IT governance and on IT-related risks, senior management should nevertheless focus on all of the risks that the enterprise may face, IT-related and others. Management should endeavor to identify all possible risks that may impact the success of the enterprise, ranging from the larger or more significant risks to the overall business down to the less major risks associated with individual projects or smaller business units. A risk identification process requires a studied, deliberate approach for looking at potential risks in each area of operations and then identifying the more significant risk areas that may impact each operation in a reasonable time period. The idea is not to just list every possible risk but to identify those that might impact operations with some level of probability and within a reasonable time period. This can be a difficult exercise because we often do not have a good understanding of the probabilities of the risk occurring or the nature of the consequences if the enterprise has to face the risk.

Some enterprises have a chief risk officer function that should have an ongoing responsibility for the enterprise risk management function. Otherwise, senior management should build an informal or formal risk management team to manage their risk management processes. The team should represent all significant elements of the enterprise and include members from internal audit, legal, and key management offices to lead in risk management activities.

The risk management team's risk identification process should occur at multiple levels in an enterprise. A risk that impacts an individual business unit or project may not have a great impact on the entire enterprise or beyond. Conversely, a major risk that impacts the entire economy will flow down to the individual enterprise and its separate business units. Some major risks are so infrequent but still can be so cataclysmic that it is difficult to identify them as a possible future event.

A good way to launch an enterprise-wide risk identification process is to begin with a high-level enterprise organization chart that lists corporate-level as well as operating units. Each of those units may have facilities in multiple global locations and also may consist of multiple and different types of operations. Each separate facility will then have its own departments or functions. Some of these separate facilities may be closely connected to one another, while others represent little more than corporate financial reporting investments. A difficult and sometimes complicated task, an enterprise-wide initiative should be launched to identify all risks in various individual areas. This type of exercise can sometimes gain interesting and/or troubling results. For example, corporate-level management may be aware of some product liability risks, but a frontline supervisor in an operating unit may look at the same risks with an entirely different perspective.

Members of the enterprise at different levels will look at some of these same risks from different viewpoints. A marketing manager may be concerned about competitor pricing strategies or the risk of pricing activities that would put the enterprise in violation of restraint-of-trade laws. An IT manager may be concerned about the risk of a computer virus or malware attack on application systems but will have little knowledge of those same pricing issue risks. More senior management typically will be aware of a different level and set of risks than would be on the minds of the operations-oriented staff. Still, all of these risks should at least be identified and considered on a unit-by-unit basis and over the entire enterprise.

To be effective, this risk identification process requires much more than just sending out an e-mail to all operating units with a request to list the key risks in their operating units. This type of request will typically result in a wide range of inconsistent answers with no common approach. A better approach is to identify people at all levels of the enterprise who would be asked to serve as risk assessors. Within each significant operating unit, key people should be identified from operations, finance, IT, and unit management. Their goal would be to identify and then help assess risks in their units built around a risk identification model framework. This is the type of initiative that can be led by an enterprise-wide risk management group, if one exists, or an internal controls assessment function such as internal audit.

An effective approach here is to outline some high-level "straw man" risk areas that may impact various operating units. Knowledgeable people can then look at these hypothetical risks and expand or modify them as appropriate. Exhibit 8.1 shows such a sample enterprise risk model framework. It lists some major risk areas that may impact an enterprise, such as strategic, operations, and finance risks. This is the type of high-level list that a CEO might jot down in response to an annual stockholders' meeting question such as, "What worries you at the end of the day?" Certainly not listing all risks facing the enterprise, this is the type of first-pass list that an enterprise can use to get started on a detailed identification of risks. The people responsible in the enterprise—often the designated risk management team—can meet with senior management and ask some of these "What worries you . . ." types of questions to identify such high-level risks.

This very general, high-level risk model can serve as a basis to better define the specific risks facing various units of an enterprise. For example, the model lists "Business Continuity Risks" under "Technological Risks." An IT manager should be able to expand this to a long list of detailed technology-related risks associated with business disaster recovery and continuity. An operations manager who is the user of IT resources might look at business continuity risk from a very different perspective and introduce other new risks associated with what happens if IT services are not available. In order to have a better understanding of the risks facing an enterprise, it is often best to expand these lists to establish a more complete set of risks.

Quantitative or Qualitative Risk Assessments

A very important step in the risk assessment process is to take all of the identified risks and to rank them in terms of their significance and likelihood of occurring. There are

EXHIBIT 8.1 Types of Enterprise Business Risks

Strategic Risks

External Factors Risks	Internal Factors Risks
■ Industry Risk ■ Economy Risk ■ Competitor Risk ■ Legal and Regulatory Change Risk ■ Customer Needs and Wants Risk	■ Reputation Risk ■ Strategic Focus Risk ■ Parent Company Support Risk ■ Patent/Trademark Protection Risk

Operations Risks

Process Risks	Compliance Risks	People Risks
■ Supply Chain Risk ■ Customer Satisfaction Risk ■ Cycle Time Risk ■ Process Execution Risk	■ Environmental Risk ■ Regulatory Risk ■ Policy and Procedures Risk ■ Litigation Risk	■ Human Resources Risk ■ Employee Turnover Risk ■ Performance Incentive Risk ■ Training Risk

Finance Risks

Treasury Risks	Credit Risks	Trading Risks
■ Interest Rate Risk ■ Foreign Exchange Risk ■ Capital Availability Risk	■ Capacity Risk ■ Collateral Risk ■ Concentration Risk ■ Default Risk ■ Settlement Risk	■ Commodity Price Risk ■ Duration Risk ■ Measurement Risk

IT Systems and Infrastructure Risks

Financial Risks	Operational Risks	Technological Risks
■ Accounting Standards Risk ■ Budgeting Risk ■ Financial Reporting Risk ■ Taxation Risk ■ Regulatory Reporting Risk	■ Pricing Risk ■ Performance Measurement Risk ■ Employee Safety Risk	■ Information Access Risk ■ Business Continuity Risk ■ Availability Risk ■ Infrastructure Risk

many formal and often mathematically complex approaches that can be used here, but since we are not analyzing a government-funded power plant or the like, an enterprise is often best off with using a simple and straightforward risk assessment approach that will be understood and accepted by all members of the senior management team responsible for its risk management process.

As just discussed, the enterprise and its business operating units should first identify all significant risks facing all aspects of the enterprise. The exercise of assembling such a list often produces a wide variety of potential risks, some of which are often beyond the understanding or appreciation of senior management. An IT manager, for example, may highlight a risk in the enterprise's IT service-oriented architecture strategy, as introduced in Chapter 13, that an enterprise executive may not understand or appreciate. The IT function can argue the significance of that risk and why more resources are needed to address it. However, senior management must have a consistent approach for looking at such risks and the related costs of installing corrective actions. They then must balance that risk against the many others that may have been identified.

While there are many formal published approaches to a formal risk analysis process, an enterprise needs a simple but thorough approach looking at all of the identified

risks to decide which of those require corrective actions and monitoring. A variety of approaches can be used, ranging from a relatively quick best-guess qualitative approach to some detailed, very mathematical quantitative approaches. The whole idea here is to help management to better decide which of a series of potentially risky events should give enterprise management the most to worry about.

A simple but often effective approach is to take the list of identified risks previously discussed and circulate them back to all participants, identifying the risks or others with a questionnaire asking for each risk:

- What is the likelihood of this risk occurring over the next one-year period? Using a score of 1 to 9, assign a best-guess single-digit score as follows:
  - Score 1 if you see almost no chance of that risk happening during the period.
  - Score 9 if you feel the event will almost certainly happen during the period.
  - Score 2 through 8 depending on where you feel the likelihood falls between these two ranges.
- What is the significance of the risk, in terms of cost to the enterprise? Again using a 1-to-9 scale, scoring ranges should depend on the financial significance of the risk to the enterprise. A risk whose costs could lower enterprise earnings per share by perhaps one cent might qualify for the maximum score of 9.

Questionnaires for this simplified approach should be independently circulated to knowledgeable people to rate or score each of the identified risks per these two measures. As an example, assume that an enterprise has identified six risks, R-1 through R-6. For each of these risks, members of the risk assessment team would be asked to separately evaluate each risk in terms of likelihood and significance. These scores are then averaged by both factors and are plotted on a risk assessment analysis chart, with four quadrants, as shown in Exhibit 8.2. R-1 had an average likelihood score of about 3.75 and a significance score of 7.00, and this score is plotted in quadrant I of the example risk assessment analysis chart. This shows R-1 as a risk that is relatively significant but not very likely to occur.

All of the identified risks should be plotted in this manner. The high-likelihood and more significant risks that end up in quadrant II should receive immediate management

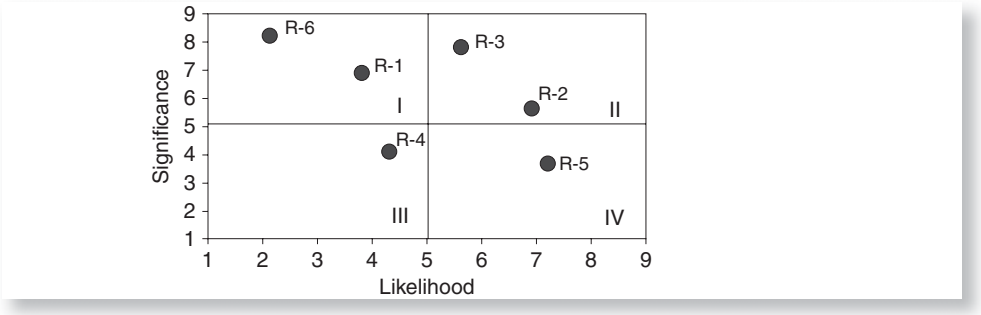

EXHIBIT 8.2 Risk Assessment Analysis Chart

attention. The ranges here of 1 to 9 are very arbitrary; the enterprise should set some relative guidelines, but staff members should just rate matters in terms of how they view the relative likelihood and significance of the identified risks. This risk assessment analysis chart provides a good qualitative measure to understand significant risks surrounding an enterprise.

The risk assessment process just described works quite well when an enterprise has identified a relatively small number of risks. It is fairly easy to look at the risk assessment analysis chart and focus on the high-likelihood and significant risks in the upper-right-hand quadrant (II) to focus on remediation planning for those risks. Often, however, if an enterprise has identified a much larger set of identified risks and ranges of 1 to 9 as well as plots on the example chart, the chart will not provide sufficient detail. A better approach then is to express these significance and impact estimates in terms of a two-digit number representing the percentage estimate (e.g., 72 percent) of achieving some risk, or as a probability (e.g., 0.72).

Simply increasing the number of digits, from just 7 or a full 72 percent, does not increase the accuracy of the assessment, but it does suggest that the risk assessment team should devote more attention to accurate estimates. It also helps assessment teams to better understand the relationship between probabilities covering independent and related events.

An accurate risk assessment process, however, requires more than just "top of the head" estimates, whether stated in a single 1-to-9 range or as a full two-digit percentage. The risk assessment team and other interested persons should take a hard look at the risks that were identified during the risk identification process and should gather more information, if necessary. For example, during the risk identification process, one manager may have identified the consequences of a new tariff law as a serious risk. Others in that same session may have expanded on that supposed upcoming law as a significant risk. However, before ranking it in terms of significance and impact, the team or other responsible mangers may want to do a bit more research to determine the actual consequences. It may be something that is not at all applicable to the unit in question or that does not go into effect until some years into the future. The point here is that all identified risks may need some additional information before they can be accurately assessed.

Risk Response Planning

There is little value in publishing detailed lists of significant risks unless the enterprise has at least taken some preliminary action steps if or when it incurs a risk. The idea is to estimate the cost impact of incurring some identified risk and then to apply that cost to the risk factor probability of the risk to derive an expected value of the risk. This is also an important time to identify a risk owner, the person or entity responsible for recognizing and monitoring the status of a specific risk. This is often an exercise that does not require detailed cost studies with lots of supporting historical trends and estimates. Our risks were identified through a rapid response brainstorming approach without detailed analysis, and likelihood and significance estimates are then made by knowledgeable people with general knowledge of an area. Expected costs also should be performed by frontline involved people at various levels of the enterprise who would be expected to have some knowledge.

The idea is to go through each of the identified risks—or if time is limited, only the key risks—and estimate the costs of incurring the designated risk. Exhibit 8.2 shows six sample risks plotted by their estimated likelihood and significance. The joint probability products of significance and likelihood become a risk score, and are ranked such that the highest value becomes the greatest item of risk concern.

The risk assessment team should look at the cost impact of each of its identified risks and estimate the total cost to the enterprise if the risk were to occur. There are many ways to develop such cost estimates, but the approach should be the same for all identified risks. The product of the risk score and the cost impact becomes the expected cost or loss to the enterprise if the identified risk occurs. The example chart shows that even though risk R-5 has the highest probability of occurring, the higher cost impact R-2 might cause a much greater management concern.

This sample risk analysis is certainly not precise, but it illustrates the type of thinking needed to estimate the costs of recovering from some risk event. It is often easy to identify some risk event, but often much more difficult to determine what it would cost to recover from that risk. As suggested throughout this chapter, there is no need to perform detailed, time-consuming analyses here but rather to ask knowledgeable people who understand the risk area to give some estimates. Teams at the entities that could incur these identified risks should make their cost estimates on the basis of:

- What is the best-case cost estimate if it is necessary to incur the risk? This is an assumption that there will be only limited impact if the risk occurs.
- What would a sample knowledgeable person estimate for the cost?
- What is the expected value or cost of incurring the risk? This is the type of risk that might include some base costs as well as such other factors as additional labor requirements.
- What is the worst-case cost of incurring the risk? This is an "if everything goes wrong" type of estimate.

We have suggested using these estimates as a starting point to get some idea of the ranges of costs in various people's thinking. However, we emphasize that this is just a high-level approach. Senior management should work with their risk assessment support staffs to understand the processes that are in place for the enterprise.

Exhibit 8.3 is an example of risk ranking planning. The "Expected Value" cell is just the product of the "Cost Impact" and the "Risk Score" cells. This number estimates what it will cost an enterprise to incur some risk. Although the numbers selected for these samples are arbitrary, they show how managers or an ERM specialist should interpret or act on this type of analysis.

Risk R-3, for example, has a high likelihood and significance as well as fairly high expected cost to correct. This is the type of risk that management should identify as a candidate for corrective actions. However, the next risk on the schedule, Risk R-2, also belongs in the upper left of the quadrant but with a relatively high cost to implement. This may be the type of risk where management decides whether to accept the risk or to develop some other form of remediation plan as discussed next.

EXHIBIT 8.3 Risk Ranking Response Planning Example

Identified Risk	Significance Probability	Likelihood Probability	Risk Score (P x I)	Rankings	Cost Impact	Expected Value of Risk Loss
R-3	8.0	5.7	45.6	1	$120,600	$ 5,499,360
R-2	5.5	7.0	38.5	2	$785,000	$30,222,500
R-5	3.9	7.2	28.1	3	$ 15,000	$ 421,200
R-1	6.8	3.8	25.8	4	$ 27,250	$ 704,140
R-4	4.2	4.3	18.1	5	$ 52,350	$ 945,441
R-6	8.4	2.0	16.8	6	$ 1,200	$ 20,160

Risk is another with a high cost to implement. Here, the significance of the risk is fairly high but the likelihood of occurrence quite low. These are the kinds of numbers where management will frequently decide to "hope for the best" and live with the risk. For this risk, it will be expensive if management incurs the risk but also expensive to install corrective action facilities. Assuming the ERM team has done a good job in preparing these estimates of identified risks, this can be a useful approach for making ongoing risk remediation decisions. R-2

Risk Monitoring

While it is important to survey the potential risks in an enterprise environment and then to estimate the costs and probabilities of those risks occurring, this cannot be a onetime exercise. Formal risk monitoring processes should be installed to test the status of these, as well as potentially new risks, on an ongoing basis. Risk monitoring is the process of identifying and analyzing the status of currently identified risks as well as keeping track of potential new risks in case they arise. It ensures that the resources that the company puts aside for a project are operating properly.

This concept of installing monitoring tools will arise in many of the other IT governance processes discussed in subsequent chapters. For example, Chapter 14 discusses IT governance and IT portfolio management, while Chapter 16 introduces the reader to effective project and program portfolio management. In those cases, and others, an enterprise needs to install monitoring controls to assess ongoing status.

In the past, many such monitoring tools did not really exist in many classic systems areas such as IT. IT staffs too often kept their fingers crossed, hoping that things were working and key systems would not fail. When they did, there was always a massive scramble to get them up and working again. It has only been in recent years that many better IT applications are installed and implemented with monitoring tools to highlight problem situations.

We have had much better experience with monitoring tools in a risk management environment. The classic wall-mounted fire alarm or door-installed burglar alarm are classic risk monitoring systems. Through the use of management dashboard–like reports or other mechanisms, an enterprise should install monitoring systems to check

the current status of identified key risks as well as alarms to signal when corrective actions need to be taken. While a senior manager generally will not be building or designing such monitoring tools, that same executive should be in a position to ask questions about the status of an enterprise's risk monitoring tools.

COSO ERM DEFINITIONS AND OBJECTIVES: A PORTFOLIO VIEW OF RISK

Chapter 4 discussed the COSO internal control framework and its importance as both a tool and measure for assessing enterprise internal controls and strengthening IT governance. As a similar but different tool, COSO ERM is a framework that will help enterprises to have a consistent definition of what is meant by enterprise-level risk that should be considered across an entire enterprise in a consistent manner. The COSO organization launched ERM in a manner similar to the development of their earlier internal control framework. An advisory council of members from the sponsoring enterprises was formed and PricewaterhouseCoopers (PwC) was contracted to develop and draft the framework description. Published in September 2004, the pages following in this chapter summarize COSO ERM concepts. However, the reader is encouraged to also access the entire description of COSO ERM. A full copy of COSO ERM and some supporting summary materials can be either downloaded or purchased through the AICPA or the COSO Web site at www.coso.org.

Just as the COSO internal control framework started by proposing a consistent definition of its subject, the ERM framework starts by defining enterprise risk management as follows:

> Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Since this is an almost academic-sounding definition, one should perhaps just consider and remember the key points of COSO ERM, including:

- **ERM is a process.** Though "process" is an often misused expression, the dictionary defines it as a set of actions designed to achieve a result. However, this definition does not provide help for many professionals. The idea to remember is that a process is not a static procedure such as the use of an employee badge that is designed and built to allow only certain authorized persons to enter a locked facility. Such a badge procedure—like a key to a lock—merely allows or does not allow someone entry to the facility. A process tends to be a more flexible arrangement. In a credit approval process, for example, acceptance rules are established with options to alter them given other considerations. An enterprise might bend the credit rules for an otherwise creditworthy customer who is experiencing a short-term problem. ERM is that type of process. An enterprise often cannot define its risk management

rules through a small, tightly organized rulebook. Rather there should be a series of documented steps to review and evaluate potential risks and to take action based on a wide range of factors across the entire enterprise.

- **The ERM process is implemented by people in the enterprise.** An ERM will not be effective if it is only implemented through a set of rules sent in to an operating unit from a distant corporate headquarters, where those corporate people who drafted the rules may have little understanding of the various decision factors surrounding them. The risk management process must be managed by people who are close enough to that risk situation to understand the various factors surrounding that risk, including its implications.
- **ERM is applied by setting of strategies across the overall enterprise.** Every enterprise is constantly faced with alternative strategies regarding a vast range of potential future actions. Should the entity acquire another complementary business or just build internally? Should it adopt a new technology in its manufacturing processes or stick with the tried and true? An effective ERM should play a major role in helping to establish those alternative strategies. Since many enterprises are large with many varied operating units, ERM should be applied across that entire enterprise using a portfolio type of approach that blends a mix of high- and low-risk activities.
- **The concept of risk appetite must be considered.** Risk appetite is the amount of risk, on a broad level, that an enterprise and its individual managers are willing to accept in their pursuit of value. Risk appetite can be measured in a qualitative sense by looking at risks in such categories as high, medium, or low; alternatively, it can be defined in a qualitative manner. An understanding of risk appetite covers a wide variety of issues that will be discussed further in Chapter 10 on governance and IT security risks as well as referenced in subsequent chapters on implementing IT governance. The basic idea is that every manager and, collectively, every enterprise should have some levels of appetite for risk. Some will accept risky ventures that promise high returns, while others prefer more guaranteed-return low-risk ventures. One can think of this appetite-for-risk concept or measure in terms of two hypothetical investors. One may prefer very low-risk but typically low-return money market or index funds, while another may invest in small-cap start-up technology stocks.
- **ERM provides only reasonable, not positive, assurance on objective achievements.** The idea here is that an ERM, no matter how well thought out or implemented, cannot provide management or others with any assured guarantee of outcomes. A well-controlled enterprise, with people at all levels consistently working toward understood and achievable goals, may achieve those objectives period after period—even over multiple years. However, an unintentional human error, an unexpected action by another, or even a natural disaster can occur. The December 2004 Indian Ocean tsunami[1] is an example of such an unexpected event. The last recorded major tidal wave in that part of the world took place some 400 years previously. Despite an effective ERM process, an enterprise can experience such a major and totally unexpected failure. Reasonable assurance does not provide absolute assurance.

- **An ERM is designed to help attain the achievement of objectives.** An enterprise, through its management, should work to establish high-level common objectives that can be shared by all stakeholders. Examples, as cited in the COSO ERM documentation, are such matters as achieving and maintaining a positive reputation within an enterprise's business and consumer communities, providing reliable financial reporting to all stakeholders, and operating in compliance with laws and regulations. The overall ERM program for an enterprise should help it to achieve those objectives.

ERM-related goals and objectives are of little value unless they can be organized and modeled together in a manner that management can look at the various aspects of the task and understand—at least sort of—how they interact and relate in a multidimensional manner. This is the real strength of the COSO internal control framework model; it describes, for example, how an enterprise's compliance with laws and regulations impacts all levels of internal controls, from monitoring processes to the control environment, and how that compliance is important for all entities or units of the enterprise. In a similar manner, COSO has developed an ERM framework model that provides some common definitions of risk management as well as helping to achieve key risk objectives throughout the enterprise.

COSO ERM FRAMEWORK

The COSO internal control framework, as discussed in Chapter 4 and described in Exhibit 4.1, has become a worldwide model that does a very effective job of describing and defining internal controls. Perhaps because some of the same team members were involved with both the internal controls and risk management project, the COSO ERM framework—at first observation—looks very similar to COSO internal controls. The COSO ERM framework shown in Exhibit 8.4 is a three-dimensional cube with the components of:

- Four vertical columns representing the strategic objectives of enterprise risk.
- Eight horizontal rows or risk components.
- Multiple levels of the enterprise, from a "headquarters" entity level to individual subsidiaries. Depending upon the enterprise, there can be many "slices" of the model here.

This section will highlight some of the horizontal components of COSO ERM. A more detailed description of COSO ERM and its three-dimensional components, as well as how they all relate to one another, can found through www.coso.org as well as in this author's more detailed description of COSO ERM.[2] The ERM framework provides a model for enterprises to consider and understand their risk-related activities at all enterprise levels as well as how those activities impact one another. As part of an understanding of IT governance, an objective of this book is to help senior managers to better understand and manage the risks facing their enterprises.

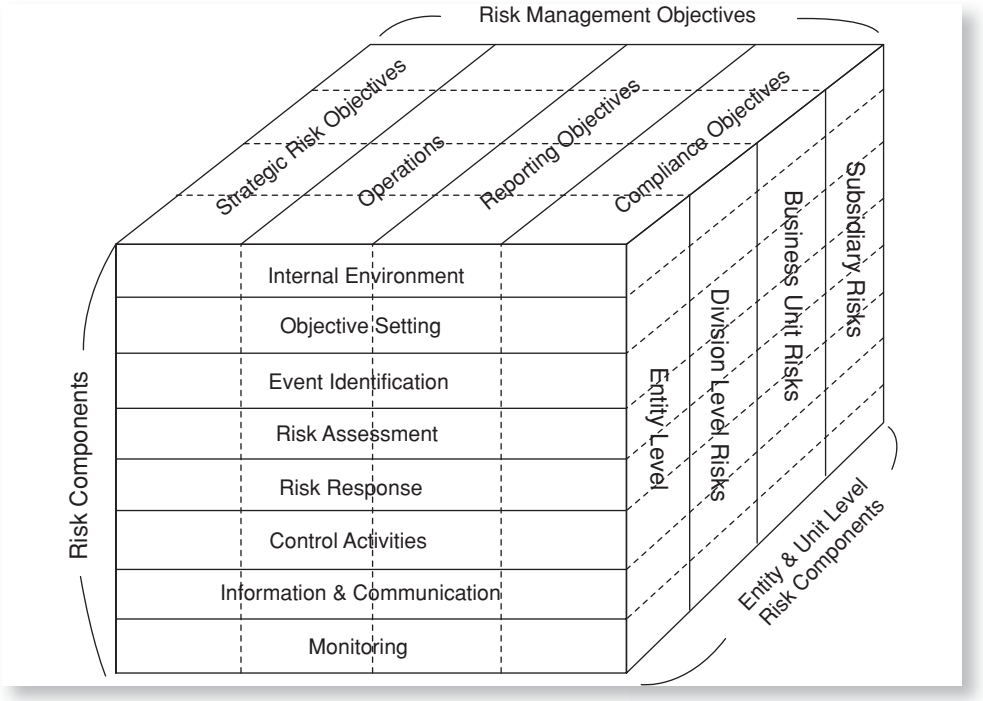

EXHIBIT 8.4 COSO ERM Framework

The COSO ERM framework description looks very similar to the COSO internal control framework that has become familiar to many professionals. When COSO ERM was first released, some initially incorrectly viewed it as just a new update to their more familiar COSO internal control framework. However, looks can be deceiving; COSO ERM has different objectives and uses! COSO ERM is not just a new and improved or revised version of the COSO internal control framework. It is much more. The following paragraphs will outline this framework from a risk components and risk management objective-setting perspective. Our objective is to introduce COSO ERM with a focus on how ERM can improve IT governance practices within an enterprise.

COSO ERM Components: Internal Environment

As illustrated in Exhibit 8.4, an element called the internal environment is placed at the top of components in the COSO ERM framework. Using some old terminology, the internal environment may be thought of as the capstone to the COSO ERM framework. Going back to the ancient era of bridges constructed of bricks, the capstone was a stone that held together the brick arches rising from each side of a span to hold the overall bridge together. This capstone component is also similar to the box at the top of an organization chart that lists the chief executive officer (CEO) as the designated head of the function. This level defines the basis for all other components in an enterprise's ERM model, influencing how strategies and objectives should be established, how risk-related

business activities are structured, and how risks are identified and acted upon. The ERM internal foundation component consists of the following elements:

- **Risk management philosophy.** This is the shared attitudes and beliefs that characterize how the enterprise considers risk in everything it does. While often not the type of message published in a code of conduct, a risk management philosophy is the kind of attitude that will allow senior managers and others at all levels to respond to some high-risk proposal with an answer along the lines of, "No, that's not the kind of venture our company will be interested in." Of course, an enterprise with a different philosophy might respond to this same proposal with an answer along the lines of, "Sounds interesting—what's the expected rate of return?" Neither response is really wrong, but an enterprise should try to develop a consistent philosophy and attitude as to how it accepts risky ventures.
- **Risk appetite.** A concept unfamiliar to many managers, risk appetite is the amount of risk an enterprise is willing to accept in the pursuit of its objectives. This appetite for risk can be measured in quantitative or qualitative terms, but all levels of management should have a general understanding of it as well as the overall enterprise's risk appetite.
- **Board of directors' attitudes.** The board of directors has a very important role in overseeing and guiding an enterprise's risk environment. The independent, outside directors in particular should closely review management actions, ask appropriate questions, and serve as a check-and-balance control for the enterprise. When a strong senior enterprise officer has an "it can't happen here" attitude when considering the possible risks surrounding some new endeavor, members of the board are often the best people to ask the hard questions about how the enterprise would react to a can't-happen event that happens.
- **Integrity and ethical values.** This ERM internal environment element requires much more than just a published code of conduct; it calls for strong integrity and standards of behavior for members of the enterprise. There should be a strong corporate culture that guides the enterprise, at all levels, in helping to make risk-based decisions.
- **Commitment to competence.** Competence refers to the knowledge and skills necessary to perform assigned tasks. Management decides how these critical assigned tasks will be accomplished through developing appropriate strategies and assigning the proper people to perform these often strategic tasks. We have all seen enterprises that do not have this type of commitment. Senior management will make grand and loud plans to accomplish some goal but often will make no positive effort to achieve that goal. The stock market often punishes such activities.
- **Organizational structure.** An enterprise's organization structure should have clear lines of authority and responsibility along with appropriate lines of reporting. A poorly constructed organization structure makes it difficult to plan, execute, control, and monitor activities. Every professional has seen situations where an enterprise structure does not allow appropriate lines of communication.
- **Assignments of authority and responsibility.** This assignment is the extent or degree to which levels or slices of authority and responsibility are assigned or

delegated to various groups and functions in an enterprise. The trend in many enterprises today is to push such matters as levels of approval authorities down the enterprise structure, giving first-line employees greater authorization and approval authority. A related trend has been to "flatten" enterprises by eliminating middle management levels. These enterprise structures usually encourage employee creativity, faster response times, and greater customer satisfaction. This type of customer-facing enterprise requires strong procedures that outline the "rules" for all members of the staff as well as ongoing management monitoring of these actions so that decisions can be overruled if necessary. All individuals in the enterprise should know how their actions interrelate and contribute to the overall objectives of the enterprise.

- **Human resource standards.** An enterprise's practices regarding employee hiring, training, compensating, promoting, disciplining, and all other actions send messages to all members of the enterprise regarding what is favored, tolerated, or forbidden. When management winks at or ignores some "gray area" activities rather than taking a strong stand, that message is often quickly communicated to others throughout an enterprise.

The internal environment component of COSO ERM has two major outputs that feed other elements of the COSO ERM framework: the enterprise's risk management philosophy and its relative appetite for risk. While we have discussed risk management philosophy in terms of board of directors' attitudes and human resource policies, among others, risk appetite is often a softer measure where an enterprise has determined that it will accept some risks but reject others in terms of their likelihood and impact. Exhibit 8.5 shows a risk appetite map illustrating the range where an enterprise should accept risks in terms of their likelihood and impact. This map diagram says that an enterprise may be willing to get involved in a high-negative-impact project if there

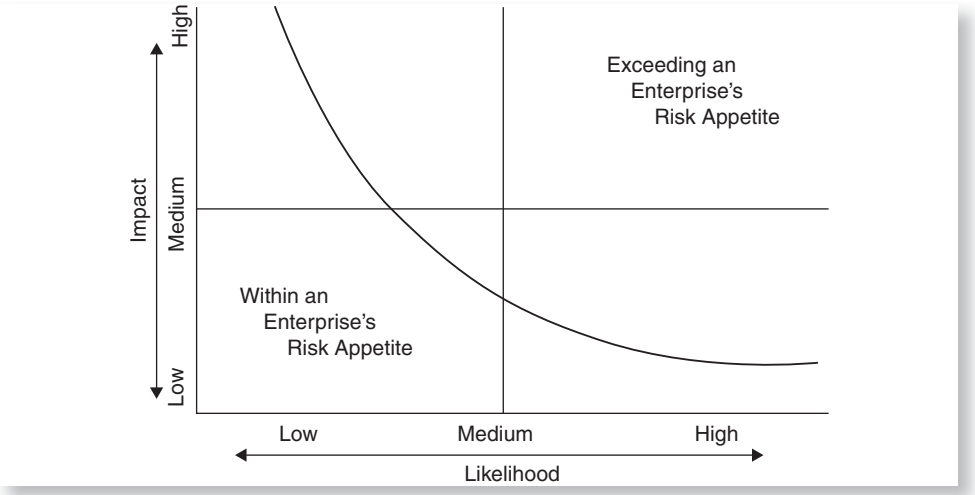

EXHIBIT 8.5 Risk Appetite Map

is a low likelihood of an occurrence. There is a third dimension to this chart as well. An enterprise will sometimes have a greater appetite for a more risky endeavor if there is a higher potential return.

COSO ERM Components: Objective Setting

Ranked just below the internal environment, COSO ERM's objective setting component outlines some necessary preconditions that must be established before management can establish an effective enterprise risk management process. In addition to the internal environment outlined earlier, an enterprise must establish high-level objectives covering its operations, reporting, and compliance activities.

COSO ERM calls for a mission statement, a general, formalized statement of purpose that can become a building block for the development of more specific functional strategies. A mission statement describes the organization's purpose, its objectives, and overall attitudes toward risks. Properly done, a mission statement will help an enterprise to select, develop, and implement a series of operations, reporting, and compliance objectives.

The internal environment component of COSO ERM, discussed previously, has two principal outputs: first, an understanding and definition of the enterprise's risk management philosophy, and second, recognition of the enterprise's risk appetite. These two outputs allow the objective setting component to develop a series of objectives to achieve risks as well as to formally define that risk appetite in terms of its tolerances for risk. Tolerances here are formal guidelines or measures that an enterprise should use—at all levels—to assess whether it will accept risks. Establishing and enforcing risk tolerances can be very difficult for enterprises. There will be problems if the rules are not clearly defined, well understood, and strictly enforced. It is often difficult to enforce rules. For example, in March 2005, the Boeing board terminated its CEO because of a "consensual relationship" with a female employee.[3] This type of relationship has often been "winked at" in the past but was recognized here as a violation of code-of-conduct rules, and the board took swift and decisive action. If an enterprise wants to establish a strict set of rules, it should be enforced throughout the entity.

A better approach for an enterprise is to establish some acceptable forms of risk tolerance. That is, they might establish a tolerable range of risks they will accept. For example, all products coming off of the production line might have acceptable preestablished error rates of less than some value. An enterprise's production line, for example, may seek to produce goods at an error rate no greater than 0.005 percent. That is an extremely low error rate in many areas, and production management in that case would accept the risk of any product warranty claims or damage to their reputation if there were errors within that very narrow limit. Of course, the ranges for an enterprise involved in health-care products would be infinitely tighter.

The point here is that an enterprise should define its risk-related strategies and objectives. Within those guidelines, it should decide on its appetite and tolerances for risk. That is, what level of risks is it willing to accept, and given those risk tolerance rules, how much is it willing to deviate from these preestablished measures? Exhibit 8.6 outlines the relationship of these COSO ERM objective setting components that might

be used for a mid-size manufacturing enterprise. Starting with an overall mission, the approach is to (1) develop strategic objectives to support accomplishment of that mission, (2) establish a strategy to meet objectives, (3) define any related objectives, and (4) define risk appetites to complete that strategy. This chart was adapted from published COSO ERM guidance materials.[4] In order to manage and control risks at all levels, an enterprise needs to set its objectives and define its tolerances for having to engage in risky practices and for its adherence to these rules. Things will not work, however, if the enterprise just establishes some risk-related objectives but then proceeds to ignore them.

COSO ERM Components: Event Identification

Events are internal or external enterprise incidents or occurrences that affect the implementation of an ERM strategy or the achievement of its objectives. While the tendency is to think of such events in a negative sense—determining what went wrong—they can be positive, negative, or both. There is a strong level of performance monitoring taking place in many enterprises today, but that monitoring process tends to emphasize such matters as costs, budgets, quality assurance, compliance, and the like. The ERM risk objectives, discussed previously, can become lost in this process of monitoring more operational and process-oriented operational objectives. Enterprises usually have strong processes to monitor such events as favorable and particularly unfavorable

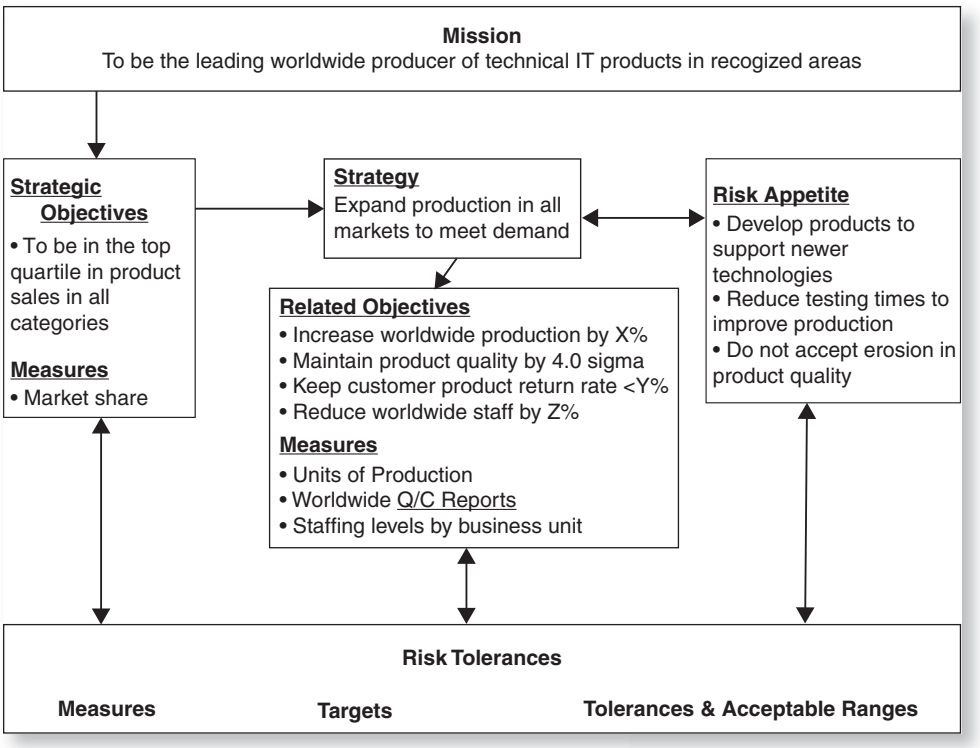
Mission
To be the leading worldwide producer of technical IT products in recogized areas
Strategic Objectives
• To be in the top quartile in product sales in all categories
Measures
• Market share
Strategy
Expand production in all markets to meet demand
Related Objectives
• Increase worldwide production by X%
• Maintain product quality by 4.0 sigma
• Keep customer product return rate <Y%
• Reduce worldwide staff by Z%
Measures
• Units of Production
• Worldwide Q/C Reports
• Staffing levels by business unit
Risk Appetite
• Develop products to support newer technologies
• Reduce testing times to improve production
• Do not accept erosion in product quality
Risk Tolerances
Measures
Targets
Tolerances & Acceptable Ranges

EXHIBIT 8.6 COSO ERM Risk Objective Setting Components

budget variances, but often do not regularly monitor either the actual events or the influencing factors that are the drivers of such budget variance events. Some of the influencing factors that should be part of COSO ERM's event identification component include:

- **External economic events.** Ongoing short- and long-term trends may impact some elements of an enterprise's strategic objectives and thus have an impact on its overall ERM framework. As an external economic event example, on May 6, 2010, U.S. and worldwide stock markets experienced massive losses in what was known as a Flash Crash.[5] Markets soon recovered, but the event caused many to take hasty and often not well-thought-out remedial actions. This was a totally unexpected external economic event.
- **Natural environmental catastrophes.** Numerous events, such as fires, floods, or earthquakes, can become incidents in ERM risk identification. Impacts here may include loss of access to some key raw material, damage to physical facilities, or unavailability of personnel.
- **Political events.** New laws and regulations as well as the results of elections can have significant risk event–related impacts on enterprises. Many larger enterprises have a government affairs function that reviews developments and lobbies for changes. However, such functions may not always be aligned with ERM objectives.
- **Social factors.** While an external event such as an earthquake is sudden and arrives with little warning, most social factors changes are slowly evolving events. These include demographic changes, social mores, and other events that may impact an enterprise and its customers over time. As an example of societal change, the previously referenced dismissal of a major corporation CEO for a consensual sexual relationship with another company employee would probably have been ignored in another era. Changing social mores today led to that dismissal.
- **Internal infrastructure events.** Enterprises often make benign changes that trigger other risk-related events. For example, a change in customer service arrangements can cause major complaints and a drop in customer satisfaction. Strong customer demand for a new product may cause changes in plant capacity requirements and the need for additional personnel.
- **Internal process–related events.** Similar to infrastructure events, changes in key processes can trigger a wide range of risk identification events. As with many such items, risk identification may not be immediate, and some time may pass before the process-related events signal the need for risk identification.
- **External and internal technological events.** Every enterprise faces many ongoing technological events that will trigger the need for formal risk identification—some gradual over time while others are more sudden. The World Wide Web has been with us for some time and the shift to an Internet environment has been somewhat gradual for many. In other cases, the growth of social network computing systems, discussed in Chapter 21, has had a major impact on enterprises in terms of relationships with their stakeholders and reputations.

An enterprise needs to clearly define what it considers are significant risk events and then should have processes in place to monitor all of those various potentially

significant risk events such that the enterprise can take appropriate actions. This is really a forward-thinking type of process that is often difficult to recognize in many enterprises.

The process of looking at the various internal and external potential risk events and deciding which events require further attention can be difficult, but COSO ERM offers some help here, suggesting that an enterprise establish some formal processes to review potentially significant risks and then to begin the process of taking action. Following COSO ERM guidance, an enterprise may consider some of the following approaches:

- **Event inventories.** Enterprise management should review other risk-related events common to an enterprise's specific industry and functional area. That is, an enterprise should consider establishing some type of "lessons learned" archive source. This is the type of data that has historically been supplied by longer-tenure members of an enterprise who can offer "We tried this several years ago, but . . ." types of comments. This type of history is often lost in today's enterprises, but an effective risk management function can provide some help here.
- **Facilitated workshops.** An enterprise can establish cross-functional workshops to first discuss potential risk factors that may evolve from various internal or external events and then develop action plans to correct the potential risks. This is one of those suggested approaches that sounds good, but most enterprises typically will not allocate their precious time to meet in cross-functional groups to talk about risks in a "What would happen if . . ." type of format.
- **Interviews, questionnaires, and surveys.** Information regarding potential risk events can come from a wide variety of sources, such as comments on customer satisfaction letters, comments from social media systems, or exit interview comments from departing employees. There is a need to capture and classify information in order to identify any that might point to a risk event. These types of responses will help to build an enterprise risk management culture.
- **Process flow analysis.** The COSO ERM application techniques supporting materials recommend the use of flow diagrams to review processes and to identify potential risk events. For many enterprises, the process flow diagrams are very similar to the internal control documentation that should have been prepared and updated as part of their SOx Section 404 documentation work, where internal controls and any control weaknesses are identified. These processes are discussed in Chapter 2 on the Sarbanes-Oxley Act.
- **Leading events and escalation riggers.** Enterprise management should establish a series of business unit objectives, the measurement criteria necessary to meet those objectives, and risk tolerance criteria to promote remedial action. For example, an enterprise's IT group may establish an objective to maintain strengthened security controls over IT network intrusions. With a measure of the number of intrusion attempts identified during a period, a threshold of over perhaps three intrusions in a given month would trigger further action. There are very good software tools available today called dashboards[6] to monitor all aspects of enterprise performance. Often very complex, such applications operate similarly to the controls on the dashboard of an automobile, where indicators will flash signals for such

conditions as low oil pressure or engine overheating. The idea is to report on risk status through some simple, easy-to-comprehend graphics, such as the common up or down arrows or red, yellow, and green traffic light logos.

- **Loss event data tracking.** While the dashboard approach just introduced monitors risk events as they happen, it is often valuable to put things in perspective after the passage of some time. Loss event tracking refers to using both internal and public database sources to track activity in areas of interest. These sources can cover a wide variety of areas ranging from leading economic indicators to internal equipment failure rates. Again, an enterprise should install effective risk identification processes to track both internal and external risk-related events.

The risk identification tools and approaches just discussed can yield some very valuable and useful information to an enterprise that identifies either risks, opportunities, or a combination of both. The key is the need for good analyses of the data as well as initiating plans for action, whether to shield from the risk or to take advantage of potential opportunities.

COSO ERM Components: Risk Assessment

We have talked about the internal environment component as being the cap or cornerstone of the COSO ERM framework, with the monitoring component as a foundation component to support the framework. The risk assessment component is about in the center of the framework and represents the core of COSO ERM. Risk assessment allows an enterprise to consider the effect that potential risk-related events may have on an enterprise's achievement of its objectives. These risks should be assessed from two perspectives: the likelihood of the risk occurring, and its potential impact. As a key part of this risk assessment process, management also needs to consider two key concepts: inherent risk and residual risk:

1. **Inherent risk.** As defined by the U.S. government's Office of Management and Budget, inherent risk is the "potential for waste, loss, unauthorized use, or misappropriation due to the nature of an activity itself." Major factors that affect the inherent risk of any activity within an enterprise are the size of its budget, the strength and sophistication of the group's management, and simply the very nature of its activities. Inherent risk is outside the control of management and usually stems from external factors. For example, the major retailer Walmart is so large and dominant in its markets that it faces a certain level of various inherent risks due to its sheer size.
2. **Residual risk.** This is the risk that remains after management responses to risk threats and countermeasures have been applied. There will virtually always be some level of residual risk.

These two concepts imply that enterprise management will always face some risks. After they have addressed the risks that came out of the risk identification process, they will usually still have some residual risks to remedy, such as a variety of inherent risks where they can do little. Walmart, for example, can take some steps to reduce its

market dominance–related inherent risks, but it can do essentially nothing regarding the inherent risk of a major natural earthquake in an operations area.

Likelihood and impact are two other key components necessary for performing risk assessments. Likelihood is the probability or possibility that the risk will occur and is often stated in terms of high, medium, or low likelihood of the risk occurring. There are some good quantitative tools here as well, but it does little good to estimate the likelihood of a risk occurring in terms of multiple decimal points if there was no basis for developing that precise a number beyond a normal statistical calculation.

Estimating the impact if a risk event occurs is a bit easier. An enterprise can develop some relatively accurate estimates of such matters as the cost of replacing facilities and equipment, the cost of restoring some system, and to some extent the cost of lost business due to the failure. However, the whole concept behind ERM is not to develop precise, actuarial-level calculations regarding the risk but to gain some measure to provide for an effective risk management framework. An analysis of risk likelihoods and potential impacts can be developed through a series of qualitative and quantitative measures. The basic idea is to assess all of the identified risks and to rank them in terms of likelihood and impact in a consistent manner.

COSO ERM Components: Risk Response

Having assessed and identified more significant risks, the next step is to determine how to respond to these various identified risks. This is a management responsibility to perform a careful review of estimated risk likelihoods and their potential impacts and, with consideration given to associated costs and benefits, to develop appropriate risk response strategies following any of four basic approaches:

1. **Avoidance.** This is a strategy of walking away from the risk—such as selling a business unit that gives rise to the risk or exiting from a geographic area of concern. The difficulty is that enterprises often do not drop a product or walk away until after the risk event has occurred. Unless there is a very low appetite for risk, it is difficult to walk away from a business area or product line just on the basis of a potential future risk if all is going well at the present in other respects. Avoidance can be a potentially costly strategy if investments were made to get into an area with a subsequent pull-out to avoid the risk.
2. **Reduction.** Business decisions may be able to reduce certain risks. Product diversification may reduce the risk of too strong of a reliance on one key product line. Splitting an IT operations center into two geographically separate locations will reduce the risk of some catastrophic failure. There are a wide range of often effective strategies to reduce risks at all levels that go down to the mundane but operationally important step of cross-training employees.
3. **Sharing.** Virtually all enterprises as well as individuals regularly share some of their risks by purchasing insurance to hedge or share them. Many other techniques are available here as well. For financial transactions, an enterprise can engage in hedging operations to protect from possible price fluctuations. A common example of hedging is the investor's use of put or call options to cover strong price movements.

It can also share potential business risks and rewards through joint venture agreements.

4. **Acceptance.** This is the strategy of no action, such as when an enterprise "self-insures" some risk rather than purchasing an insurance policy. Essentially, an enterprise should look at a risk's likelihood and impact in light of its established risk tolerance and then decide whether to accept that risk. For the many and varied risks that approach an enterprise, acceptance is often the appropriate strategy for some risks.

Management should develop a general response strategy for each of its risks using an approach built around one of these four general strategies. In doing so, it should consider the costs versus benefits of each potential risk response to best align them with the enterprise's overall risk appetite. For example, an enterprise's recognition that the impact of a given risk is relatively low would be balanced against a low risk tolerance that suggests that insurance should be purchased to provide a potential risk response. For many risks, appropriate responses are obvious and almost universally understood. An IT operation, for example, should spend the time and resources to back up its key data files and implement a business continuity plan.

An enterprise, at this point, should go back to the several risk objectives that have been established as well as the tolerance ranges for those objectives. Then it should readdress both the likelihood and impact associated with each of the identified risks within those risk objectives to develop an assessment of both of those risk categories as well as an overall assessment of the planned risk responses and how those risks will align with overall enterprise risk tolerances. At this point in the risk assessment process, an enterprise should assess the likelihood and potential impact of each of the risks surrounding its objectives, as well as some estimates for each, with a next step to develop a set of potential risk responses. This is perhaps the most difficult step in building an effective COSO ERM program framework. It is comparatively easy to identify a 5 percent likelihood risk that there will be a fire in the scrap materials bin and then to outline a risk response to install a nearby fire extinguisher. However, the responses to most risks are much more complex and require fairly detailed risk response plans.

The enterprise should initially go through its key high-impact and high-likelihood identified risks and develop a series of risk response plans. However, this can be a challenging management process. While it is relatively easy, following our earlier example, to install a fire extinguisher to provide protection from a scrap materials bin fire, things are usually not that simple. The point here is that the process of developing risk responses requires a significant amount of planning and strategic thinking in itself. The several risk response alternatives involve costs, time, and detailed project planning. In addition to the planning and strategic thinking, this risk response planning process requires significant management input and approval to recognize the various alternative risk responses and to have action plans in place to satisfy the appropriate responses.

COSO ERM calls for risks to be considered and evaluated on an entity or portfolio-wide basis and evaluated and assessed for each individual business unit or division by department, by function, and similar approaches to look at an enterprise's risks. Risks should then be summarized on their impact and frequency of occurrence, as shown in

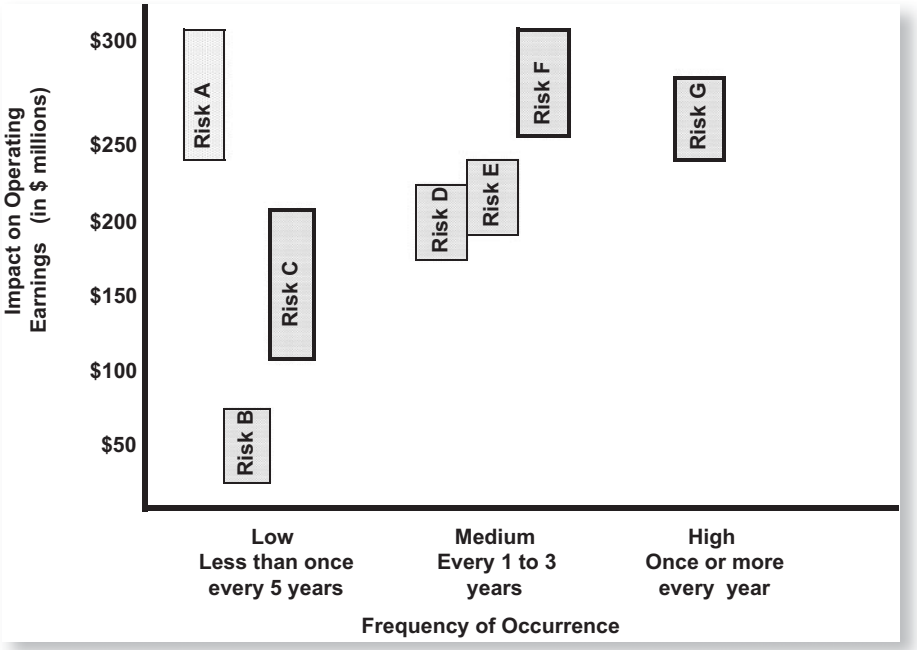

EXHIBIT 8.7 Portfolio View of Risk Summary

Exhibit 8.7. This is the type of communication that should help senior management and the board of directors to understand the portfolio of risks facing an enterprise.

COSO ERM Components: Control Activities

COSO ERM control activities are the policies and procedures necessary to ensure that identified risk responses are carried out. Although some of these activities may only relate to an identified risk and approved risk response in one area of the enterprise, they often overlap across multiple functions and units. COSO ERM control activities should be tightly linked with the risk response component previously discussed.

Having selected appropriate risk responses, enterprise management should select the control activities necessary to ensure that those risk responses are executed in a timely and efficient manner. The process of reviewing whether control activities are performing properly is very similar to processes exercised as part of SOx Section 404 internal control assessments[7] and discussed in Chapter 2. The COSO ERM risk event–risk response activities can be executed with the following steps:

1. Develop a strong understanding of the identified significant risks and develop control procedures to monitor or correct for those risks.
2. Create testing procedures to determine if those risk-related control procedures are working effectively.
3. Perform tests of the control procedures to determine if the risk monitoring process tested is working effectively and as expected.

4. Make adjustments or improvements as necessary to improve risk monitoring processes.

This four-step process is essentially what enterprises subject to the requirements of SOx have been doing to review, test, and then assert that their internal control processes are working adequately. A major difference here is that an enterprise *is legally required* to comply with SOx procedures in order to assert the adequacy of its internal controls to its external auditors. There are no such legal requirements with COSO ERM. An enterprise should seek to install risk monitoring control activities to assess the various risks it has identified. Because of the critical nature of many risks to an enterprise, risk management monitoring can be very critical to an enterprise's overall health due to the nature of the various risks it may encounter.

Many control activities under COSO internal controls are fairly easy to identify and test due to the accounting nature of many, and generally include the following:

- **Separation of duties.** A very basic internal controls concept; the person who initiates a transaction should not be the same person who authorizes that transaction.
- **Audit trails.** Processes should be organized such that final results can be easily traced back to the transactions that created those results.
- **Security and integrity.** Control processes should have appropriate control procedures such that only authorized persons can review or modify them.
- **Documentation.** Processes should be appropriately documented.

These control procedures, and others, are fairly well recognized and applicable to all internal control processes in place in an enterprise, and they also somewhat apply to many risk-related events. Many senior managers can easily define some of the key controls necessary in many business processes. For example, if asked to identify the types of internal controls that should be built into an accounts payable IT system, many professionals would identify as significant control points that checks issued from the system must be authorized by different persons, that accounting records must be in place to keep track of the checks issued, and that the check issuing process should be such that only authorized persons can initiate such a financial transaction. These are generally well- and widely understood control procedures. An enterprise often faces a more difficult task in identifying control activities to support its enterprise risk management framework.

As was discussed, as part of the ERM event identification component, management need to think of these risk categories in terms of major risk areas of operations, such as revenue, purchasing, capital spending, and information systems. Specific risk-related control activities can be defined within each of these categories, whether for the overall enterprise or covering some unit or function. Although there is no accepted or standard set of enterprise risk management control activities at this time, the COSO ERM documentation suggests several areas as follows:

- **Top-level reviews.** While senior management may be somewhat oblivious to the "do the debits equal the credits?" internal control procedures that are covered by

their financial teams and auditors, they should be very aware of the identified risk events within organizational units and should perform regular top-level reviews of the status of identified risks as well as the progress of risk responses. This type of regular review coupled with appropriate top-level corrective actions is a key ERM control activity.

- **Direct functional or activity management.** In addition to the top-level reviews outlined, functional and direct unit managers should have a key role in risk control activity monitoring. This is particularly important in a large, diverse enterprise where control activities should not just take place at a local unit level and then bump up the organizational hierarchy to some central management level. Rather, risk-related control activities should take place within the separate operating units, with communications and risk resolution taking place across enterprise channels.
- **Information processing.** Whether it be IT systems processes or softer forms such a paper or messages, information processing procedures represent a key component in an enterprise's risk-related control activities. Appropriate control procedures here, with an emphasis on an enterprise's IT processes and risks, are discussed in greater detail in Chapter 14 on implementing integrated systems.
- **Physical controls.** Many risk-related events involve physical assets such as equipment, inventories, securities, and physical plant facilities. Whether it is physical inventories, inspections, or plant security procedures, an enterprise should install appropriate risk-based physical control activity procedures.
- **Performance indicators.** The typical modern enterprise today employs a wide range of financial and operational reporting tools. Many of these tools can be used as is or modified to support risk event–related performance reporting. In many instances, an enterprise's overall performance tools can be modified to support this important control activity component.
- **Segregation of duties.** This is a classic control activity, whether for business process internal controls or for risk management. The person who initiates certain actions should not be the same person who authorizes or approves those actions. This key controls activity is important whether it be in a smaller business unit where an employee's supervisor would be required to inspect and approve employee actions or with a CEO who should obtain the oversight approval of the board of directors.

These COSO ERM control activities can be expanded to cover other key areas. Some will be specific to individual units within the enterprise, but each of them, singly and collectively, should be important components of supporting the enterprise's ERM framework.

COSO ERM Components: Information and Communication

Although described as a separate component in the Exhibit 8.1 COSO ERM framework diagram, the component of information and communication describes a set of tools and processes linking other COSO ERM components. COSO ERM's information and communication component links together each of the other components in the COSO ERM framework. Exhibit 8.8 shows the information and communication flows across

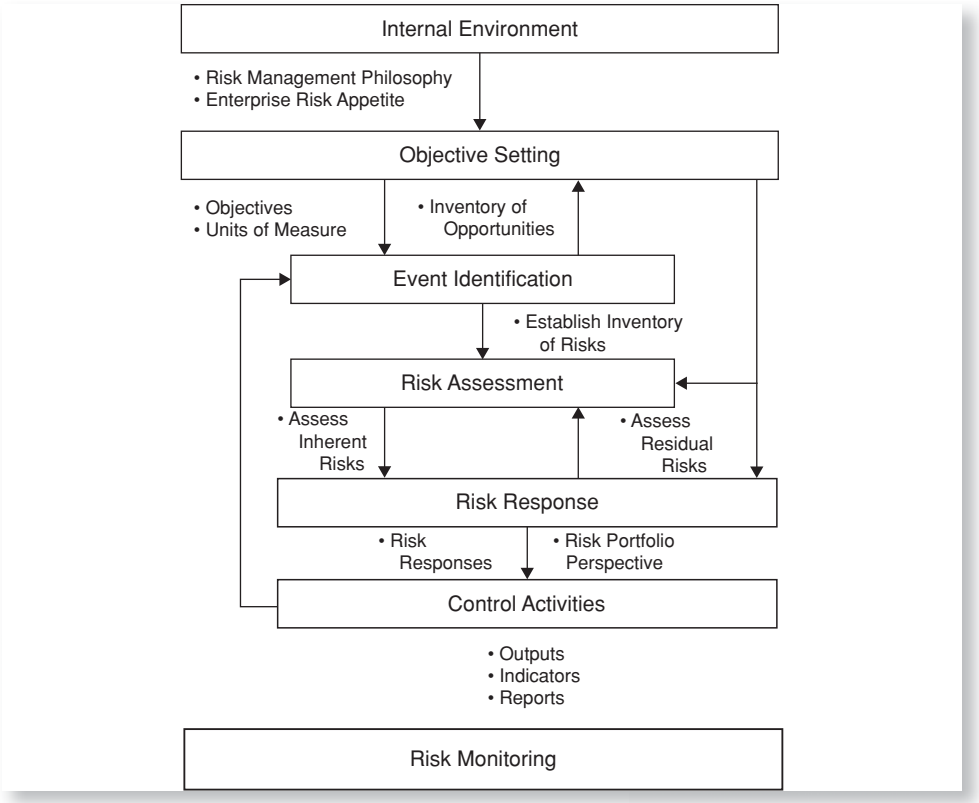

EXHIBIT 8.8 Information and Communication Flows across ERM Components

the other COSO ERM components. For example, the risk response component receives residual and inherent risk inputs from the risk assessment component as well as risk tolerance support from the objective setting component. ERM risk response then provides risk response and risk portfolio data to control activities as well as risk response feedback to the risk assessment component. Standing alone, the monitoring component does not have a direct information connection but has overall responsibility for reviewing all of these functions.

While it is relatively easy to draw such a simple flow diagram of how information should be communicated from one COSO ERM component to another, this is often a far more complex process of linking various systems and information paths together. Many enterprises have a complex web of often not very well linked information systems for their basic operational and financial processes. These linkages become even more complex with attempts to link various ERM processes given that many basic enterprise applications do not directly lend themselves to risk identification, risk assessment, and risk response processes.

An enterprise risk management initiative will be of little value unless a message on the importance of this ERM initiative gets communicated to all enterprise stakeholders. This often should be in the form of a message from the CEO. The idea is to communicate

the message about the importance of ERM throughout the enterprise. These types of messages are particularly valuable when an enterprise wants to deliver a message, for example, that all stakeholders should be very cautious regarding taking on certain potentially risky ventures. The process is more difficult if the enterprise wants to communicate that some factors should let go a little and occasionally accept some risks. An incorrectly interpreted message can effectively open the floodgates in inappropriate, risky decisions and ventures.

COSO ERM Components: Monitoring

Placed at the base of the stack of horizontal framework components, COSO ERM monitoring is necessary to determine that all elements of an installed ERM continue to work effectively. People in the enterprise change as well as do supporting processes and both internal and external conditions. In order for all members of the enterprise to have a level of assurance that their installed ERM is working effectively on a continuous basis, ERM monitoring should be installed and activated.

Ongoing and continuous monitoring processes can be an effective method to flag exceptions or violations in the overall ERM process. In order to establish an effective ERM framework, that monitoring should be expanded to include ongoing reviews of overall ERM processes ranging from identified objectives to the progress of ongoing ERM control activities. COSO ERM monitoring could include the following types of activities:

- Implementation of a strong and ongoing management reporting mechanism such as cash positions, unit sales, and other key financial and operational data. A well-organized enterprise should not have to wait until fiscal month-end or worse for these types of operational and financial status reports. Reporting tools should be expanded to include key ERM measures, including some form of flash reporting taking place at all appropriate levels of the enterprise.
- Periodic reporting processes should be installed to monitor key aspects of established risk criteria, including such things as acceptable error rates or items held in suspense. Rather than just reporting periodic statistics, such reporting should emphasize risk-related alerts such as statistical trends and comparisons with prior periods.
- Current and periodic status reporting of risk-related findings and recommendations from internal and external audit reports.
- Updated risk-related information from sources such as government revised rules, industry trends, and general economic news. Again, this type of economic and operational reporting should be available for managers at all levels.

Separate or individual evaluation monitoring refers to detailed reviews of individual risk processes by a qualified reviewer, such as an internal audit function. Here the review can be limited to specific areas or cover the entire ERM process for an organizational unit. In this latter type of review, qualified outside consultants may be hired to assess the effectiveness of ERM in the entire enterprise. However, for many enterprises, a strong internal audit enterprise may be the best internal source to perform such specific ERM

reviews. Whether it is internal audit, outside consultants, or trained staff from within the enterprise, any specific individual reviews of an ERM process might use the following tools:

- **Process flowcharting.** As part of any identified ERM process, the parties responsible should develop flowcharts documenting their ERM processes. This requires looking at the documentation prepared for a process, determining if the process documentation is correct given current conditions, and updating the process flowcharts as appropriate.
- **Reviews of risk and control materials.** An ERM process often results in a large volume of guidance materials, documented procedures, report formats, and the like. There may often be value for a dedicated ERM team, internal audit, or the enterprise's quality assurance function to review the risk and control materials from an effectiveness perspective.
- **Benchmarking.** Benchmarking here is the process of looking at another's ERM functions to assess their operations and to develop an approach based on the best practices of others. Gathering such comparative information is often a difficult task as competing enterprises are often reluctant to share competitive data. The process works best when one-to-one professional contacts can be developed, and information regarding how others have attempted to solve similar problems is often very valuable.
- **Questionnaires.** A good method for gathering information from a wide range of people, questionnaires can be sent out to designated stakeholders with requests for specific information. This is a valuable technique for monitoring when the respondents are scattered geographically, such as a risk monitoring survey of employees in a nationwide retail enterprise.
- **Facilitated sessions.** Valuable information can often be gathered by asking selected people to participate in a focus group session led by a skilled conference leader. This is the approach used by many enterprises for gathering market research information through what are called focus groups. This same general approach can be used to gather a team of people—often from different positions in the enterprise—to review the enterprise risk status of a particular area.

The purpose of this monitoring process is to assess how well the ERM framework is functioning in an enterprise. Deficiencies should regularly be reported to the managers responsible for enterprise risks in the specific area monitored as well as to the ERM or risk management office. The concept behind COSO ERM monitoring is not just to find faults or deficiencies but to identify areas where the ERM framework can be improved.

OTHER DIMENSIONS OF THE COSO ERM FRAMEWORK

As discussed at the beginning of this chapter and described in Exhibit 8.1, COSO ERM is a three-dimensional framework with its eight categories as one dimension in the sections just discussed. The other two dimensions are its four objective categories represented by its vertical columns, and its entity and units described in the

third dimension. While the eight ERM categories just described are very important to understanding and using COSO ERM, those other two dimensions of strategies and organizational units are important as well. To understand the risks surrounding an organizational objective, one must evaluate that risk in terms of, possibly, the reporting concerns associated with that risk and the specific organizational unit that becomes the main focus of the risk.

COSO ERM needs to be understood from all three of these ERM framework dimensions. An effective ERM process, no matter how well designed and operated, only provides reasonable—but not positive—assurance that the enterprise will achieve its risk-related objectives within management's established philosophy and appetite for risk. However, no matter how well an ERM is designed and managed, there can be failures due to human errors or risk events caused by any of a wide range of unexpected events.

THE OCEG GRC "RED BOOK," RISK MANAGEMENT, AND IT GOVERNANCE

The OCEG is an industry-led nonprofit organization that develops standards and helps enterprises enhance their governance, risk management, and compliance processes. With major support from the technical industry, the OCEG has developed and published a GRC capability model, called the OECG "Red Book," with IT governance standards that is becoming increasingly well recognized in many enterprises worldwide.

With its emphasis on IT governance, this section reviews the OCEG Red Book GRC capability model guidance materials. While many of these guidance materials are very similar to other GRC and ERM framework guidance information found here and in other chapters, we feel that the OCEG will have a significant impact on IT governance and GRC processes in future years.

OCEG's use of "open" in its title has some special meaning in an IT sense. An open system regularly exchanges feedback with its external environment to continuously analyze that feedback, adjust internal systems as needed to achieve the system's goals, and then transmit necessary information back out to that environment. Closed systems, unlike open systems, have hard boundaries through which little information is exchanged. Organizations that have closed boundaries often can become stagnant and unhealthy. Closed-system examples include bureaucracies, monopolies, and stagnating systems. A common term in many newer, advanced IT systems today, *open* is an appropriate word for this GRC capability model.

The OCEG's GRC guidance is found in a document called the Capability Model Red Book and is located at www.oceg.org. The basic document, dated April 2009 at the time of our publication, is available through the Internet, while an enhanced version is available to subscribing members. The basic edition contains a complete description of this GRC model, but at an additional cost an enhanced version with templates and other help aids is also available. The capability model is based around a concept called Principle Performance®, an integrated GRC approach that we will discuss in the sections following.

The OCEG GRC capability model has many concepts here that are very similar to COSO ERM and other GRC concepts discussed in other chapters, and include the following objectives:

- Enhance general business objectives
- Enhance organization culture
- Increase stakeholder confidence
- Prepare and protect the enterprise
- Prevent, detect, and reduce adversity
- Motivate and inspire desired conduct
- Improve responsibility and efficiency
- Optimize economic and social value

OCEG's Principled Performance® Concept

OCEG has obtained a trademark for this term and uses this concept to describe the need for an articulation of an enterprise's financial and nonfinancial objectives to achieve all of the objectives an enterprise chooses to pursue while employing an effective, efficient, and responsive approach to supporting governance, risk management, and compliance objectives. The concept here is that all enterprises must operate within defined external and internal boundaries where outside forces, such as legal and regulatory requirements, establish the mandated external boundaries. The objective is to integrate GRC principles and objectives to help an enterprise more effectively drive performance.

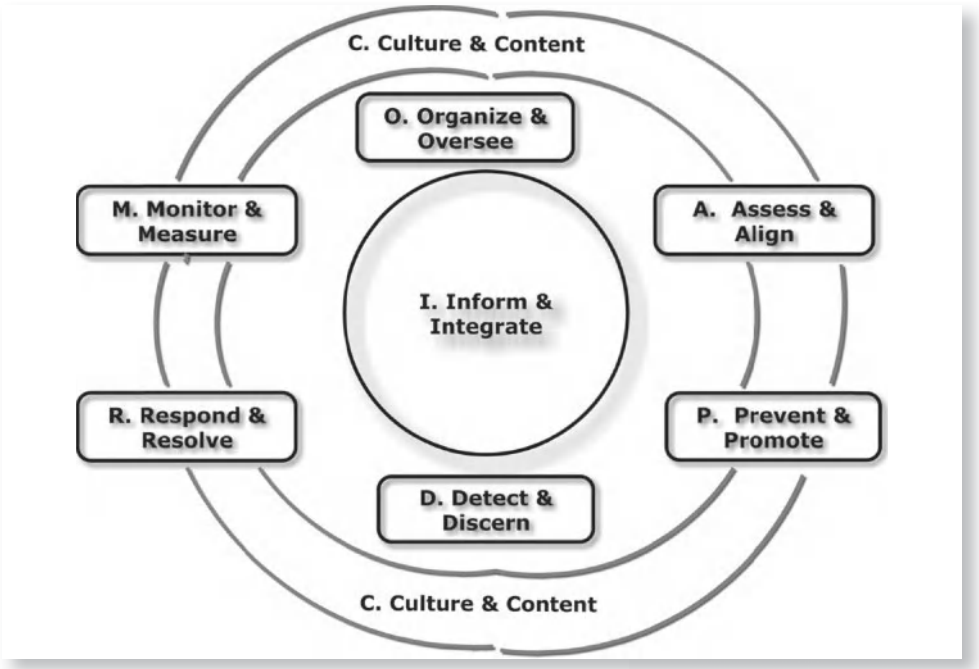
C. Culture & Content
O. Organize & Oversee
M. Monitor & Measure
A. Assess & Align
I. Inform & Integrate
R. Respond & Resolve
P. Prevent & Promote
D. Detect & Discern
C. Culture & Content

EXHIBIT 8.9 OCEG GRC Capability Model

For an enterprise to achieve the concept of principled performance, it must clearly define its mission, vision, and values and define the objectives it seeks to achieve. It must define how it will pursue these objectives while also addressing risks and uncertainty, protecting and creating value, identifying new opportunities, and staying within defined boundaries of ethical conduct. The enterprise should make these choices transparent to appropriate internal and external stakeholders and attempt to accomplish all of this using an integrated approach to achieve highest possible levels of performance.

In order to achieve the OCEG's Principled Performance, every entity or unit in an enterprise must define what is "right" for it and then do these right things in the right way. We have paraphrased this concept from the OCEG materials, a high-level objective that goes beyond traditional concepts of enhancing shareholder value to include desired outcomes that address enterprise stakeholder interests.

These Principled Performance concepts are key elements of the OCEG's GRC capability model as shown in Exhibit 8.9. The following sections briefly describe the elements of that model in greater detail, particularly when they have different goals and objectives than in the conventional COSO ERM framework described earlier in this chapter. This model outlines a very high-level set of materials and concepts that are part of the OCEG model. The interested reader is encouraged to access the full model through our previously referenced Web address.

Each entry on the OCEG model is supported by GRC elements and sub-elements. For example, the letter *C*, or Culture and Content, element is supported in the OCEG documentation by four elements:

C1 External Business Context
C2 Internal Business Context
C3 Culture
C4 Values and Objectives

Each element of the GRC capability model then reduces down to subelements for each. For example, for C3 or Culture, the model contains the subelements:

C3.1 Analyze Ethical Culture
C3.2 Analyze Ethical Leadership
C3.3 Analyze Risk Culture
C3.4 Analyze Board Involvement
C3.5 Analyze Governance Culture and Management Style
C3.6 Analyze Workforce Engagement

Each of these is supported by more detailed elements to expand the outline. In addition, the model contains a set of principles and a list of common sources of failure for each as well as guidelines and references for additional support materials.

Similar detailed objectives are found for each of the Exhibit 8.10 elements and subelements. In addition, this model contains documented subpractices for each of the subelements. For example, the O, or Organize and Oversee, element found in the upper center has an element called O2, Roles and Responsibilities, with a subelement O2.4,

EXHIBIT 8.10 GRC Subpractices Example: O2.4 Define and Enable GRC System Operational Rules

O2.4.01 Define roles and responsibilities for the following key GRC activities:

- Methodology, policy and procedures, standards, vocabulary, and maintenance
- Risk and requirements identification, analysis, and optimization
- Initiative implementation/project portfolio management
- Stakeholder relations
- Helpline or hotline
- Investigation and resolution
- Performance measurement
- Communications, including public relations
- Information management
- Technology

Define and Enable GRC System Operational Rules. These element and subelement descriptions exist for each throughout the model. For example, Exhibit 8.10 shows the activities for O2.4.01.

Our objective here is not to describe each of these OCEG elements, subelements, and activities in detail, but to describe the general concepts behind the OCEG model. The reader can access the overall model through the Web site www.oceg.org.

With an outline of detailed sub- and sub-sub-points, there is sufficient detail here to help an enterprise establish and organize a GRC function. There are good sets of principles and common sources of guidance to help organize an effective GRC process for an enterprise. This and the preceding sections have outlined the elements of the OCEG GRC capability model on a very high level. Some are very similar to the GRC and COSO ERM processes discussed in other chapters. Others call for a more detailed and sometimes more administrative controls–oriented approach. Our high-level description, however, does not give justice to the full study that can be found in a 240-page publication in its basic form with much more detail in the extended document. The interested reader is encouraged to further investigate the OCEG GRC model.

Level and Scope of the OCEG Standards-Setting Authority

The OCEG at present does not have the IT governance standards-setting authority as found with the PCAOB or ISO. In addition, although it has released some strong guidance materials, that information still does not have the level of recognition that is found through professional standards such as those issued by the IIA or ISACA. Nevertheless, we feel that the importance of the OCEG and its guidance materials will only grow in future years and as concerns and need for effective GRC processes grow.

A major strength of the OCEG is that it is totally a volunteer organization managed by staff members on loan from its sponsoring organizations and formed into an OCEG leadership council. Sponsors here include the major public accounting firms such as PwC and Grant Thornton. In addition, there are many major IT industry leadership sponsors from such firms as Oracle and SAP as well as primarily U.S. industry sponsors

from such firms as the major insurance company Aon and the retailer Walmart. If there is any concern here, it appears that the OCEG is more of a U.S.-based and not a truly international organization, based on its sponsoring organizations and committee members. In our global world today, we need more of an international focus.

An interested senior manager may want to use this OCEG material as an additional source of reference. It is an extensive set of materials that we can only expect will grow in its importance in future years.

NOTES

1. "Tsunami Facts and Information," Australian Government, Bureau of Meterology, www.bom.gov.au/tsunami/info/index.shtml.
2. Robert R. Moeller, *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes*, 2nd ed. (Hoboken, NJ: John Wiley & Sons, 2011).
3. Christine Hauser, "Boeing Board Ousts Chief, Citing Relationship with Executive," *New York Times*, December 7, 2005.
4. *Enterprise Risk Management—Integrated Framework: Application Techniques* (COSO, April 2004).
5. Scott Patterson, "Breakdown: A Glimpse Inside the 'Flash Crash,'" *Wall Street Journal*, June 10, 2012, wsj.com/article/SB10001424052702303296604577454330066039896.html?mg=reno64-wsj.
6. Two vendors that supply dashboards are the software suppliers Business Objects and COGNOS.
7. For more information on Section 404 internal control reviews, see Robert Moeller, *Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL* (Hoboken, NJ: John Wiley & Sons, 2008).

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

PART THREE

Tools and Technologies to Manage the IT Governance Infrastructure

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER NINE

Cloud Computing, Virtualization, and Portable, Mobility Computing

THE WORLD OF IT SYSTEMS is constantly filled with ever-evolving new technologies and concepts. Some of these are IT concepts and changes that quickly become common accepted practices. The Internet language Java is an example of such a newer technology. Applications using Java have become a vehicle allowing communication between central Internet sites and individual systems, and Java has become an Internet development standard. Many other newer technologies, however, initially received much publicity in various IT publications but did not establish much of a position in the marketplace and were soon forgotten. In the end, they were "not that big of a deal" as IT consumers and the market overlooked them or competitors came up with better offerings.

Some newer technologies have been with us for quite a while now, and are only really new when compared to traditional IT systems and processes. These technologies change the way we think of building and managing IT systems and their supporting processes. This chapter will look at three such newer technologies that are becoming increasingly common in IT operations today, where each also presents some IT governance issues.

First we will discuss what has become known as cloud computing, a concept that relates to our use of the Internet and the World Wide Web since the late 1990s. Professionals today use an Internet search tool such as Google to seek answers to questions or to gather more information on some subject. While a typical search request almost instantaneously responds with a wide span of search "hits" or findings for the request, we really do not think much about how we got all of those responses so quickly. They all came from the Internet, both from our home country and abroad. Because we cannot point to a specific system or resource as the supplier of our Internet query, we tend to think of these Internet resources as a vast, interconnected telecommunications network, almost a "cloud" of resources.

IT resources, beyond just search engines, are increasingly offered through this Internet cloud. Whether it is a national or international service facility or even a large enterprise facility, we are increasingly using cloud computing to build and manage our IT systems. This chapter will discuss some IT governance issues that arise when we use this cloud for IT systems and processes.

Systems virtualization and its IT governance issues is the second technology discussed in this chapter. Although it had origins going back to earlier models of IBM mainframe systems many years ago, virtualization is a concept that was unknown to most IT business professionals until not too long ago. It goes back from when we moved from one centralized mainframe IT system first to a few and soon to many interconnected IT server systems. While it was initially easy to connect each server system to a set of storage units and other facilities, systems became more and more complex as IT systems configurations grew. In addition, IT operations management soon realized that its configurations of connected and attached server resources were not very well balanced. Server A, for example, may have a lot of attached memory or mass storage facilities but may not use all of these resources as part of its scheduled or normal operations. Another server, B, may be short and need some of server A's excess resources to help it out during higher computing load periods.

In the older days of client–server computing, these resources were connected to each separate server through specific program instructions or even physical cable connections. Making changes, such as borrowing A's unused resources to help out B, was often a time-consuming and sometimes complex task. This connection and balancing problem was solved by some of the storage management vendors starting in about the year 2000 by what is known as systems virtualization.

With virtualization, system resources are not physically connected but are logically joined through software tools. Depending on systems resource demands, separate systems can be virtually connected to other resources, in a dynamic sense, rather than using older, manual physical cable or defined software connections. Virtualization can introduce major efficiencies to a large IT installation. However, if IT systems virtualization processes are not properly understood, implemented, and managed, they can introduce some IT governance issues. This chapter will introduce IT virtualization concepts and discuss some key related governance issues.

This chapter will conclude by discussing IT governance issues surrounding the wide spectrum of personal handheld computing devices that are used not just for personal purposes but as enterprise IT system components. Small tablet computing devices or smartphones are terrific tools for communications, accessing the Internet, taking photographs, or a wide range of other tasks. Although launched as personal devices, they have made major inroads into workplaces. This chapter will conclude by discussing IT governance issues associated with personal computing devices in the workplace.

UNDERSTANDING CLOUD COMPUTING

Some older business managers, who grew up in the pencil-and-paper days, may have felt that some members of their IT systems and development staffs have had their "heads in the clouds" for years, but what is known as cloud computing is a newer and evolving

concept that is important to many IT operations. Closely related to the concepts of service-oriented architecture (SOA) discussed in Chapter 13, cloud computing is changing the way that many enterprises build and use IT applications.

The cloud metaphor is often used to refer to the Internet here and in other published references. The idea behind this Internet cloud is that users do not need knowledge of, expertise in, or control over a technology infrastructure "in the clouds" that supports Internet-based applications. The term originated in the telephone industry, where up until the 1990s, data and even early Internet circuits were hardwired between destinations. Then long-haul telephone companies began offering wireless virtual private network services for data communications. The growth of these wireless networks and the Internet and World Wide Web enhanced the way that we think of IT services today.

Cloud computing, however, is more than just the Internet. It is the way we think of the services that Internet-resident applications provide. Because it is impossible to determine in advance precisely the paths of Internet traffic, the cloud metaphor has been used to denote IT service facilities that are the responsibility of the service providers as well as the network infrastructure. The concepts of software products or services on the Internet, or SOA, soon followed.

Software vendors are increasingly offering their products as services on the Internet rather than applications that are resident on individual customer servers. A good example—and an early product type leader—is the provider of customer relationship management software SalesForce (www.salesforce.com/crm/products.jsp). This supplier of customer and sales tracking software tools does not sell its products as a set of programs loaded on proprietary CDs for customer use. Rather, all of the SalesForce programs and documentation are found on the Internet, and customers pay for their software only when they use the product. The SalesForce applications are used as a service to customers.

Exhibit 9.1 shows this cloud computing concept. We have highlighted several vendors that currently offer cloud computing products today, including Amazon, Google, and Microsoft, as well as SalesForce. This is only a limited example of some current applications, and there certainly are many more. Some of the benefits of applications in a cloud computing environment are:

- **Reduced infrastructure costs due to centralization.** With an IT application in the cloud, there is no need to maintain the same level of software change management processes and other controls for those applications in the cloud. This can be somewhat of a mixed blessing for some because you only get the features and formats that the software allows.
- **Increased peak load capacities.** Cloud providers, such as Amazon or Google, have very large IT systems server farms with massive capacities—their computer operation load capacities seem almost infinite.
- **Consistent systems performance is monitored by the provider of the service.** Cloud providers have the ability to monitor all IT services provided by the cloud vendor and significant users. As a result, the provider should have monitoring tools in place to provide process improvement changes as required.

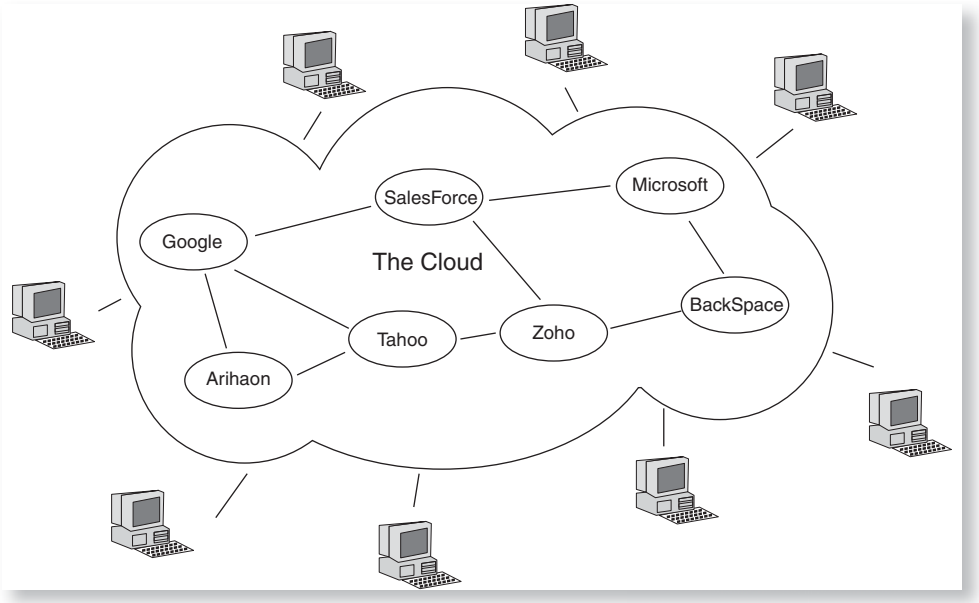

EXHIBIT 9.1 Cloud Computing Concepts

- **Application and IT services resiliency.** Cloud providers have mirrored solutions that can be utilized in a disaster scenario as well as for the load-balancing of traffic. Whether there is a natural disaster requiring a site in a different geographic area or just heavy traffic, cloud providers normally will be equipped.

Enterprise managers who are implementing IT governance need to take a different approach in reviewing internal controls for SOA applications as well as understanding IT security in a cloud computing environment. Web and other infrastructure services are increasingly being delivered in a cloud environment, and there is a need to rethink some audit and control considerations.

Reviewing Cloud Computing Application Controls

Just because an application is operating out of an SOA environment does not mean that the need to assess and understand its application internal controls goes away. The SOA-based application should continue to have the same audit trails, error-checking procedures, and other good practices that would be found with any well-controlled IT application. We can almost expect that a business application run under a major cloud vendor such as Google, often with many worldwide users, can be expected to have adequate internal controls.

Cloud computing represents a major change in the way applications are run and managed, and while there are only a limited number of vendors providing service-based software applications today, that number of service providers can be expected to increase. There is an implicit level of trust in the services provided by many vendors under these Internet clouds, but their IT and business management leaders as well as IT auditors

should gain assurances that these cloud-based applications are well controlled. The direct and indirect users of cloud computing should develop a strong level of trust in the software services and infrastructure that make up the cloud for an enterprise. The enterprise executive who determines that an IT function is adopting a cloud computing strategy for some of its applications should meet with IT management to gain an understanding of such initiatives. Some of the key cloud computing IT governance and assurance issues are:

- **Transparency.** Cloud service providers must be able to demonstrate the existence of effective and robust security controls, assuring customers that their information is properly secured against unauthorized access, change, and destruction. Key questions for any service provider offering cloud applications are:
  - What types of cloud service provider employees have access to any customer information?
  - Is a segregation of duties among cloud provider employees maintained?
  - How are the files and data for different customers' information segregated?
  - What controls are in place to prevent, detect, and react to any security and control breaches within the cloud?
- **Privacy.** Cloud computing service providers should provide assurances that privacy controls are in place that will prevent, detect, and react to breaches in a timely manner, with strong and periodically tested lines of communication.
- **Compliance.** In order to comply with various applicable laws, regulations, and standards, there can be cloud computing concerns that data may not be stored in one place and may not be easily retrievable. It is critical to ensure that if data are demanded by authorities, it can be provided without compromising other information. When using cloud services, there must be a guarantee that an enterprise can get its information when needed, or that a service provider may claim a right to withhold information from authorities.
- **Transborder information flows.** With cloud-generated information potentially stored anywhere in the cloud, the physical location of the information can become an issue. The physical location dictates jurisdiction and legal obligation. There are many legal issues here yet to be solved.
- **Certification.** Cloud computing service providers should provide their customers assurance that they are doing the "right" things. In the future, we should see independent third-party audits and/or service auditor reports that will become a vital part of any cloud computing service provider assurance program. These reports follow an AICPA standard known as SAS 70[1] that will become more important in the years going forward.

Strong and effective standards will effectively help enterprises to gain assurance about their cloud computing supplier's internal controls and security. At the time of this publication, however, there are currently no publicly available specific cloud computing standards.

With no defined set of such standards, a senior manager or an IT auditor reviewing applications provided by a cloud computing service provider should request that the service provider at least offer strong assurances in three key areas:

1. **Events.** The service provider should regularly document and communicate changes and other factors that have affected SOA system availability.
2. **Logs.** The service provider should provide comprehensive information about an enterprise's SOA application and its runtime environment.
3. **Monitoring.** Any such surveillance should not be intrusive and must be limited to what the cloud provider reasonably needs in order to run its facility.

Cloud computing represents some new and interesting opportunities to rework security and IT controls for a better tomorrow, and more formalized cloud computing standards should soon follow. We can expect to see much more in the future as cloud applications and cloud service provider computing grows and matures.

Cloud Computing Security and Privacy Challenges

The use of applications operating in a cloud computing environment shifts a wide range of challenges and responsibilities from primarily an enterprise's IT function to an environment where some responsibilities are assumed by the cloud computing service provider while others still are the responsibility of the enterprise IT function. This is a challenge for IT management and its internal auditors as well, who must understand the security and privacy components of their selected service providers.

Cloud computing is still a new and evolving trend. An increasing number of vendors are offering suites of cloud-based applications, and vendors such as Google and Amazon are building huge, multiserver cloud computer complexes, but there is not an established set of recognized best practices across these various service providers. In some respects, this trend of enterprises to shift some their in-house IT resources to cloud service providers has, in a perhaps strange sort of manner, some similar elements to the move to what is now a very much in the past concept of IT service bureaus in the early 1980s.

In the mid-to-late 1970s, many enterprises decided they needed to move from their manual or unit record punchcard processes to one of the then-new mainframe computer systems. Many added systems development programming staffs and built and implemented new mainframe computer systems, often with very disappointing results. A frequent problem was that these new mainframe systems did not have the capacity to process the needed volumes of enterprise data, and when they did, they experienced computer system maintenance or downtime problems.

A solution for many at that time was to convert and move their computer systems operations to what was called a service bureau—a larger centralized computer systems resource that collected input materials for many clients, processed their systems, and delivered the output reports. The computer systems service bureaus did not work well for everyone. Many subscribed to these services without fully realizing what they would be getting in terms of the services, integrity, and internal control monitoring for their enterprise processes. These service bureau computer operations have gone away today, even well before the demise of the mainframe. However, some of the same things happened then as today with enterprises now converting some of their conventional applications to a cloud environment. A major issue is that enterprises do not always

ask the right questions of their service providers when converting to an SOA cloud environment.

When making a decision to select a service provider as part of a move to SOA and cloud computing, an enterprise should ask any competing service provider vendors some hard questions about their operations and standards. The management team responsible for enterprise IT governance should gain assurances in some of the following seven areas and concerns in selecting a cloud computing service provider:

1. **Privileged user access.** Sensitive data processed outside an enterprise and in a cloud environment brings with it an inherent level of risk, because outsourced services in the cloud bypass conventional physical, logical, and personnel IT controls that an IT organization would exert over its in-house systems programs. The cloud service provider should provide thorough information and assurances about the people who manage an enterprise's data and systems in the cloud. Service providers should supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.
2. **Regulatory compliance.** An enterprise is ultimately responsible for the security and integrity of its own data, even when it is held by a service provider. The cloud computing service provider should supply detailed information on its security governance policies as well as reported results of its recent external audits and security certifications. In addition, it should agree to update the enterprise on these activities on a regular basis.
3. **Data location.** When an enterprise uses the cloud for key data and systems, it probably won't know exactly where data is hosted—even in which country. Because of data ownership laws, cloud service providers should identify the specific jurisdictions where they will be storing and processing the enterprise's data. The service provider also should make a contractual commitment to obey local privacy requirements on behalf of its customers.
4. **Data segregation.** Data in the cloud is typically in a shared environment alongside data from other customers. The cloud provider should provide detailed information on what is being done to segregate data at rest and also should supply evidence that its encryption schemes were designed and tested by experienced specialists. Encryption accidents can make data totally unusable and even can complicate availability.
5. **Recovery.** Even if an enterprise does not know the location of its cloud-stored data, the cloud provider should document what will happen to an enterprise's data and service in case of a disaster. The service provider should provide evidence, including test results, that their recovery methods will replicate the data and application infrastructure across multiple sites. The service should assert whether it has the ability to do a complete restoration, and how long it will take.
6. **Investigative support.** Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. A service provider should provide a contractual commitment to support specific forms of investigation,

along with evidence that the vendor has already successfully supported such activities.

7. **Long-term viability.** An enterprise has no guarantee that its cloud computing provider will never go broke or get acquired and swallowed up by a larger company. However, an enterprise should gain assurances from its cloud provider that its data will remain available even after such an event. Any service provider should provide assurances that users will get their data back in a format that they could import into a replacement application.

Cloud computing and its SOA applications are evolving and rapidly changing areas. We can expect to see more established standards and recognized best practices in future years. Even though we have made reference to the usage of IT service bureaus of many years ago as an example of how not to select a cloud service provider, we feel that there have been enough lessons learned in that regard not to repeat those mistakes. Cloud computing is a wave of the future, and we should see much more usage of this concept in the years going forward.

IT SYSTEMS AND STORAGE MANAGEMENT VIRTUALIZATION

Virtualization is the concept of pooling of IT physical storage facilities from multiple network storage devices into what appears to be a single storage device that is managed from a central console. Storage virtualization helps an IT storage administrator perform the tasks of backup, archiving, and recovery more easily, and in less time, by disguising the actual complexity of the overall network of IT storage devices. This author was first introduced to storage management virtualization around 2002 when he was part of a small consulting group at EMC Corporation that was launching an information technology infrastructure library (ITIL) consulting practice (ITIL best practices are discussed in Chapter 6). At that time, EMC was a leader in storage management devices, and its introduction of virtualization concepts was a major technology innovation. Virtualization has since become a widely used and important IT resource management process.

To understand IT virtualization, one should revisit the earlier days of computer systems—particularly the mainframes of older days. Those computers had operating systems that controlled various attached peripheral devices, including printers, tape drives, and what were then called mass storage disk and drum drive devices. Although earlier mainframe computer systems initially made massive use of the relatively inexpensive magnetic tape drives to store data, technology quickly moved to storage devices based first on rotating magnetic drums and then to disk drives. Although they were much more expensive when first introduced in the early days of IT, disk and drum drives quickly became more popular than tape drives. The limitation with tape drives was that to read the 100,000th record on a tape, the drive had to pass through the first 99,999 records to find it. Drum drives quickly became an almost historical footnote, and technology soon moved to rotating disks, which were much faster and had indexing schemes that located that 100,000th record almost instantaneously.

In general, IT virtualization means to create a virtual version of an IT device or resource, such as a server, storage device, network, or even an operating system where the framework divides the resource into one or more execution environments. Even the common personal practice of partitioning a desktop system hard drive is considered virtualization because you take one drive and partition it to create two separate hard drives. Devices, applications, and human users also are able to interact with the virtual resource as if it were a real single logical resource. The term virtualization has become somewhat of an IT buzzword, and computer systems with elements that have been virtualized are called virtual machines (VMs). IT virtualization is associated with a number of IT technologies, including the following:

- **Storage virtualization.** The amalgamation of multiple network storage devices into what appears to be a single storage unit, IT storage management virtualization was first introduced by the storage management firm EMC in about 2002, and the concept has been picked up by many hardware and storage management vendors.
- **Server virtualization.** This is the partitioning of a physical server into smaller virtual servers. IBM first developed this concept with its VM mainframe computer operating system back in the 1980s.
- **Operating system–level virtualization.** This is a type of server virtualization technology that works with complex, software-layered operating systems.
- **Network virtualization.** A single physical network can be made virtual through the logical segmentation of network resources.
- **Application virtualization.** This same concept can be used to increase IT utilization and efficiency and to manage upgrades and backups more easily, as will be discussed in the following section.

Virtualization in general is the separation of a device's functions from its physical elements through the use of specialized software. With virtualization, a unit's physical location is separated from its functions, and controlling software manages the data or functions, despite their physical location. It is a very efficient method to manage and control separate physical units through specialized virtualization software. With proper controlling software, virtualization techniques can be used for multiple IT hardware devices, including storage management, network components, servers, operating systems, or even applications.

IT virtualization today is literally taking the information technology industry by storm. Polls have indicated that over half of all larger-enterprise IT functions now are running at least one virtual server, and a far smaller but growing number have a security strategy tailored to their virtual environment. However, if an enterprise has already implemented or is in the process of implementing an IT virtualization strategy, it may be at risk for security threats that could have a significant impact on its operating environment. Since traditional security systems rely on hardware and special operating systems to protect their environment, they can be rendered useless in a virtual environment where the goal is to reduce or eliminate hardware.

In addition, traditional best practices are now in question because physical segmentation and other methods are nearly impossible to implement. And finally, due to

the nature of a virtual environment, network complexities are increasing faster than legacy management and monitoring systems, so visibility into the virtual and physical environments can be extremely cloudy. Enterprises need to take a closer look at a new means of securing their networks and sensitive information in the new virtual world.

The section following discusses some of the unique IT security issues associated with implementing IT virtualization. These are beyond the general IT security governance issues discussed in Chapter 10. In addition, virtualization can raise some unique IT governance issues. Senior managers should have an understanding of their IT function's virtualization strategy and internal control processes.

IT Governance and Virtualization

As mentioned, the concept of virtualization first appeared in the mainframe days of old when IBM introduced the concept of what they called virtual machines as an element of their 1980s mainframe computer architecture. The unique characteristics of VM machines then moved to desktop computers as we moved to client–server systems and embraced the Internet. Virtualization has become a frontline hot topic today as we virtualize storage management processes and implement VMs in the multiserver, networked systems of today.

At first, data center managers believed that they could manage those VMs in much the same way as they were managing their physical servers, but experience has shown that this is generally not possible. While there are a lot of commonalities between the two environments, there are also some significant differences that impact systems management and governance.

One of the biggest differences is the potential impact of virtualization on existing control processes and procedures. For example, a data center should have specific processes and procedures when it comes to provisioning new servers; these generally involve sign-offs and handovers between the various data center teams, eventually resulting in a new server being installed in the data center. However, an IT operation can create a new VM literally with the click of a mouse—either by copying an existing one or generating a new one from a template—and these processes become easy to bypass.

For example, enterprise IT operations can make multiple identical virtual copies of a specific server and distribute them around organization operating units; there can be governance and control challenges to keep track of them. The management systems provided by the virtualization software vendors will specify where a specific VM is at a point in time, but not where it has been, or about its relationships with other VMs. This is compounded by the fact that VMs are, by definition, mobile. They can (and do) move around the environment after they have been deployed; this movement not only makes them more difficult to track and manage but can also compromise data and application segmentation policies.

These differences, and others, also make it difficult for most existing data center management tools to operate in the virtual space and leave potential blind spots. This is further compounded by the lack of virtualization management tools, reporting, and automation. The result is a very manual environment that does not integrate well into existing data center compliance and control models. This means that traditional

"red flag" or alert systems may not be working properly in this space, and they are either being circumvented or simply not seeing the day-to-day operation, leaving your data center exposed.

In a physical IT data center, with all its associated systems, processes, and checks-and-balances, flags are raised if things move out of process. Management by exception is the rule of the day and it's an environment where "no news" is truly good news. But in an environment where the controls are predominantly manual and reporting is scarce, the lack of control visibility can create issues that IT operations management will not see coming. This may not be too much of an issue when the virtual computing environment is small, but as the environment grows, the impact of these issues grows with it.

As enterprise IT functions adopt these virtual environments, the lack of automated controls in some VM environments and the increased need for manual internal control activity may create imbalances between IT and internal control operations; this will only increase as the VM environment grows. This lack of automated controls, monitoring, and continuous measurement in the virtual data center, combined with the corresponding increase in manual processes, produces an environment that has less effective controls and more risk than its physical counterpart.

IT Virtualization Governance and Security Issues

An aggressive but poorly planned move to virtualization can create challenges for an enterprise. As we have discussed in other chapters, the more any established enterprise governance, risk, and compliance (GRC) systems move out of balance, the greater the impact to the overall business. The individual "tipping point" here will be different for each organization, but sooner or later it will be reached when organizations start to see their costs and risks escalate. A lot of enterprises may already be running into unplanned IT expenses, caused by inefficient virtual environments. Others are seeing a rise in visible and invisible data center incidents, all of which eventually impact the overall business performance.

An enterprise senior manager should discuss enterprise IT virtualization and VM strategies with IT management. If the move to VM machines appears to be almost haphazard, there should be evidence of a strong project plan, as discussed in Chapter 16, as well as a demonstrated appreciation for some of the unique control concerns associated with IT virtualization. A lot of existing operational and risk policies and control objectives still apply to the virtual world. They may have to be adjusted to fit the dynamics of this new architecture, but they still apply. These include elements common to all servers (physical or virtual), such as configuration, patch management, and security. However, virtualization has a uniqueness that requires new policies and controls, including:

- **Identity management.** Given the dynamic nature of VMs, some level of file and resource identity management will be needed that is not based on simple naming conventions. The IT quality assurance function, as well as IT internal audit, should review and assess processes to assure that policies are being applied correctly.
- **VM mobility control.** Part of the value that virtualization brings is the flexibility it provides to IT groups. VMs are designed to be mobile and are easily moved from host

to host in response to automated load-balancing processes or the manual removal of VMs from a physical host that is in need of maintenance. However, mobility can be a double-edged sword, as not all VMs should be mobile. For example, IT may need to demonstrate, for control or audit purposes, that some application conforms to regulation or internal corporate standards. Policies may be required about where specific VMs should and should not be allowed to run, as well as how long VMs should be allowed to stay offline (powered off).

- **Provisioning.** Traditional server provisioning processes can be easily circumvented in the virtual space, so new processes need to be established that control both what gets provisioned and who has the authority to authorize new servers.
- **Data separation.** Every data center has specific rules around its application data separations, usually driven by either security concerns or compliance issues. As IT virtualizes applications that fall under these standards, it's important to consider how they will enforce this on the virtual side, not just when the VM is provisioned, but also to protect against inappropriate movement throughout its life cycle, either malicious or inadvertent.
- **Reclamation.** Ensuring that redundant or unused VMs are removed in a timely fashion is another area requiring specific policy and objectives. Also, the security impacts of this new technology need to be considered: including the impact of VMs on existing security systems (some systems don't work well in the virtual space) and the potential of new attack threats.

The typical senior manager responsible for enterprise IT governance may not be familiar with the previously listed issues. However, they can be used as talking points with their IT function for an assessment of an enterprise's IT virtualization program. Server virtualization, despite its rapid worldwide adoption, is still a relatively immature technology. For many, it has entered the data center through the back door as an operations tool with a very good return on investment (ROI), and has since evolved into a new data center architecture. But entering this way, it has never been subject to the normal internal control review processes that IT functions usually go through before deployment into the data center, and lacks some much-needed functionality.

There are a number of different virtualization software platform products on the market today, with VMware as the market leader, and a few others such as Microsoft and Citrix. Each of these platforms has a different set of strengths and weaknesses, and many IT functions have ended up running a mix of all three, raising the issue of managing across heterogeneous environments. The management systems provided by virtualization vendors, not surprisingly, focus more on VM deployment than management of the environment. Additionally, most of the traditional data center management vendors whose systems are built for the physical data center don't work well in the virtualized environments.

Relying on the IT operations and GRC processes that have been discussed in other chapters, enterprise management should work with its IT operations to determine that adequate internal control standards remain in place in the virtualized environment. For many, additional systems may be needed for the "virtual data center," both to make up for the shortcomings of the existing data center management and

virtualization systems and to implement and enforce the additional policies that this space requires.

Virtualization is here to stay. If an IT function is ramping up the adoption of server virtualization in the data center, they should consider its impact on business internal controls, including:

- **Overlay existing standards and processes into the virtual space wherever possible.** Existing standards and processes will probably require tweaking, but ensuring they are in place will start to provide needed visibility and control, as well as insight into what additional management systems will be needed.
- **Establish the new standards and processes that this technology needs.** An enterprise should increase its visibility and control even further. At a minimum, these should include:
  - Monitoring and reporting
  - Provisioning control
  - VM identity management
  - Mobility controls to enforce data separation
  - Reclamation of end-of-life VMs
- **Automate as much as possible.** Manual processes are inconsistent and time-consuming. Ultimately, the only way to get an enterprise GRC model back in balance is to increase the level of automation by implementing the additional systems that this space needs. This will have the additional effect of reducing the amount of manual activity and processes, increasing internal controls, and reducing risk, as well as saving a significant amount of administration time.
- **Review your security architecture.** In order to be effective, many types of security appliances and monitoring tools need to know what they are protecting and where it is, and the mobility of VMs can be problematic. The constant change enabled by virtualization can place dynamic demands on any "static" types of security solutions, even in small virtualized infrastructures. Bottom line: Some security infrastructures will not work well in a virtualized environment, and a security product that does not work well, for all intents and practices, may not work at all.
- **Implement specific audit and internal standards (and reporting systems) for the virtual space.** As discussed, the virtualization environment requires new control policies, processes, and standards. As these come into play, they will require corresponding new internal control, audit processes, and procedures. For example, SOx-compliant applications will need to be segmented from other systems, as well as tighter access controls applied. The inherent mobility of virtual servers adds an additional factor to the audit process: Has this VM moved to an additional host during the audited period? If so, what other VMs were on that host?

As often happens with any newer IT technology, the installation of virtualization software and major changes can cause some major process efficiency improvements. However, these new tools are often installed by IT management but are too often beyond the understanding of general senior management. Senior managers at all levels should obtain a general understanding of the virtualization activities in their enterprise.

Exhibit 9.2 is a list of some virtualization IT governance good practices for a typical commercial enterprise. These should help a senior manager to better understand how virtualization is being implemented in an enterprise.

Virtualization started in most data centers as a tactical effort, led by IT, and focused on the ROI associated with server consolidation. But moving from tactical server consolidation to more production-oriented uses of virtualization, and increasing the percentage of data centers that are virtual, requires a more strategic view about the impact of this architecture on data center management and business controls. Effective virtualization processes and controls will ensure that an enterprise can optimize the overall value of this technology.

EXHIBIT 9.2 IT Governance Virtualization Good Practices

- **Make certain that all affected parties understand the advantages and disadvantages of virtualization.** Before IT migrates from older physical systems to virtual, or deploys a new fleet of virtualized servers for a specific workload, IT and management should be sure to understand the limitations and realities of virtualization in terms of CPU utilization, memory, and overall IT governance controls.
- **Establish priorities over the management, patching, and security of virtual systems.** Limit the proliferation of virtual machines, and include all virtual machines in IT's patching, management, and security policy infrastructures.
- **Treat virtual systems the same as physical systems in most circumstances.** Virtual systems should generally not be treated as any different than physical ones. Virtual systems should be implemented with a well-defined set of data governance policies and practices designed to ensure that virtual systems data is:
  - **Accessible.** Systems users should be able to access the data they need with data formats that match the user requirements.
  - **Secure.** Similar to all conventional applications, only authorized people should be allowed to access virtualized data and non-authorized users should be prevented from accessing it.
  - **Consistent**. When two users seek the "same" piece of data, is must be actually the same data, with multiple versions regularly rationalized.
  - **High-quality.** Data from virtualized applications must be accurate and conformed to meet agreed IT standards.
  - **Auditable.** In a virtual environment, there must be clear paths indicating data sources, a clear view of the data's lineage, and controls to indicate that IT knows who is using it and for what purpose.
- **Employ aggressive application backup procedures.** Backing up an entire virtual machine can take considerable time and may give few options for rapid recovery. However, IT should regularly back up virtual applications just as it protects mission-critical physical systems, making sure it has the capability to recover rapidly and reliably as well.
- **Centralize systems storage.** A leading cause of virtual machine proliferation is that host devices are often physically spread throughout an organization. With virtual systems, copying an entire guest system (or two) is easy, and this ease of duplication is a key reason for virtual machine proliferation and the potential result of data losses. If IT can't physically secure its virtual machines, it should have its virtual or physical disks encrypted to ensure no loss of confidential data. By placing your virtual machine hosts and storage in central, secure locations, IT can minimize both proliferation and the potential for data loss.

SMARTPHONE AND HANDHELD IT DEVICE GOVERNANCE ISSUES

People at all levels today are using powerful handheld smartphone devices as well as tablet computers for their personal and household activities. These started as small personal cell telephones but have expanded over the years as devices to access the Internet, send text messages, take and transmit photographs, and much more. Tablet computers have all of the capabilities of laptop computers, often with the exception of a larger keyboard, but are smaller, light in weight, and can essentially double as a smartphone. Despite their many powerful features, these devices are relatively low in cost. They have become personal devices used by many families, including smaller children. In this section, we have referenced all of these systems as handheld devices, whether smartphones, tablet computers, USB storage clips, or others.

It was not that many years ago that these handheld devices did not exist in the workplace. Enterprises encouraged their key employees to use laptop computers and issued them along with security links to access enterprise software products. However, these laptop devices were on loan for business use, their personal use was generally discouraged, and the machines were returned to the enterprise IT functions after the employee's departure.

Today, employee personal use of smartphones and tablet computers can raise some IT governance issues. For example, these devices generally have a built-in digital camera feature. This can certainly raise a security issue given that an employee can easily snap a photo of a sensitive document and then transmit and use it for improper purposes. Despite published rules prohibiting such practices, an enterprise cannot really prevent such in-house photography, despite strong policy statements against such activities. Similarly, many use small USB clips that can be plugged into a corporate device and used to capture sensitive data.

Many of the concerns about the use of handheld devices in the workplace are related to enterprise security. An enterprise will want to allow key employees to connect to corporate data networks that are part of their work responsibilities. However, firewalls, antivirus software, and security monitoring software tools need to be installed on any mobile device that will be given access to enterprise network systems. Because of the large number and types of devices available, an enterprise cannot control the issuance of such devices but must have established standards that are required for their use before accessing corporate data.

Exhibit 9.3 is an example of a corporate policy for the employee and other stakeholder use of handheld devices in a workplace environment. Such a policy should be communicated to all new employees along with a request for their formal acceptance of the policy. Because technology is always changing, the dimensions and nature of today's handheld device may be much different from what will be common tomorrow. This type of policy statement should be periodically updated and reissued, with a requirement that recipients acknowledge their understanding and acceptance of the revised policy. Key elements in this handheld policy should be used by management and internal audit as part of their regular internal control reviews.

EXHIBIT 9.3 Policy for Employee and Other Stakeholder Use of Handheld Devices

Introduction. The use of handheld devices is increasing in our corporate environments, providing mobile services and constant connectivity to mobile workers. Due to the fact that handheld devices are often the property of individuals, they present new threats to corporate assets. Handheld devices with security challenges include laptops, removable storage (e.g., USB key devices), smartphones, tablet computers, and other cameras.

Purpose and Scope. This security policy establishes rules for the proper use of handheld devices in all corporate environments in order to protect the confidentiality of sensitive data, the integrity of data and applications, and the availability of our company services. This protects handheld devices and their users, as well as corporate assets (confidentiality and integrity) and the continuity of the business (availability).

This policy applies to all employees, consultants, vendors, contractors, students, and others using business or private mobile handheld devices on any premises occupied by our company. Adherence to these requirements and the security policies derived from them and implementation of provisions is binding across the whole of our enterprise, its subsidiaries, and majority holdings. Willful or negligent infringement of the policies jeopardizes our company interests and will result in disciplinary, employment, and/or legal sanctions. These requirements and the security policies derived from them and implementation provisions also apply to all of our suppliers.

Roles and Responsibilities. All employees and stakeholders are responsible for adhering to these information security provisions. Specific tasks are documented in the definition of roles, and for each role a person must be defined by name and made known to the IT security department.

IT Governance Responsibilities.

- **Business unit owners.** Ensures the necessary resources are provided to the IT department.
- **IT management.** Maintains security policies:
  - Responsible for the creation, adaptation to existing policies in place, and maintenance to keep them up to date.
  - Implements guidelines and procedures to implement this policy and communicates them to the intended people.
  - Ensures that all applicable procedures are documented and are well communicated.
  - Is responsible for policy enforcement and ensuring that users are properly trained.
- **IT security management.** Responsible for managing all issued mobile handheld devices:
  - Manages the registered handheld device inventory.
  - Ensures that the necessary services are available to users and provides the necessary resources for the use of services.
  - Is responsible for policy enforcement:
    - Via the appropriate working controls.
    - Makes requests for changes/adaptations in this policy to support IT governance.
- **Users and other stakeholders.** Enterprise employees and other stakeholders must read, understand, and agree to these security policies and must inform IT management of exceptions to these security policies.

NOTE

1. SAS 70, "Service Auditors Reports," http://sas70.com/sas70_reports.html.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER TEN

Governance, IT Security, and Continuity Management

EFFECTIVE IT SECURITY AND CONTINUITY management processes are important elements of overall enterprise IT governance. *IT security* is a broad term that refers to processes and controls that will protect both IT systems and data, as well as the enterprise's physical assets, from a wide variety of potential threats. In our Internet-driven world of today, aside from the risk from people worldwide who might be interested in improperly accessing secured systems, IT security is an ever-present and growing concern. An enterprise needs to implement effective IT security processes that will allow it to govern and control its IT assets.

While security processes are important to protect IT assets from unauthorized persons, IT operations also face threats from such risks as fires in a facility, natural disasters, or equipment failures. This is the area of IT risk concerns that was known as IT disaster recovery planning in the early days of IT when mainframe systems were predominant; today it is generally called *IT continuity planning*. Whether it be hardware or software backup resources, an enterprise should have the resources in place to continue operations in the event of any non-normal interruption in the regular operations schedules.

This chapter discusses why it is important to have IT security and continuity processes in place for effective IT governance. Effective IT security and continuity planning processes are often complex, requiring the skills of specialists. However, the senior manager directing and reviewing the status of overall IT governance processes should have a general knowledge of some effective tools and procedures. They are each specialized areas but are important components for overall effective IT governance in the enterprise.

IMPORTANCE OF AN EFFECTIVE IT SECURITY ENVIRONMENT

IT security has very much changed and become a more complex concern over the years. Back in the days of the mainframe systems, we thought of IT security as little more than

simple password systems and locks on computer center doors. It was important that systems assets were protected and frequently backed up. Processes were the responsibility of IT operations, with little general management involvement.

Today, with frequent news releases about such IT-related events as the theft of computer system credit card files or the public disclosure of supposedly secret computer system message files, IT security issues have become a major concern for many members of IT and general enterprise management. While IT security has always been a concern going back to the earliest days, this risk area has become a much greater concern in today's world of vast Internet connections and increasing reliance on cloud computing strategies. An enterprise's audit committee and senior management are often the parties who read about IT security breaches elsewhere and question the chief information officer (CIO), the chief audit executive (CAE), and IT auditors about enterprise IT security.

Concerns regarding IT security are among the major issues impacting both general and IT management. To gain assurance about having effective IT security, an enterprise needs to establish and build a strong and well-managed IT security environment. This task is the responsibility of IT operations and enterprise management at all levels. IT management can assist in this process by implementing effective internal controls and strong security policies and procedures, and by working with all levels of the enterprise to establish an effective security environment.

This chapter will focus on building an effective IT security governance environment from three perspectives. First, there is a need to establish some strong IT systems security principles, such as were discussed in Chapter 5 on COBIT or Chapter 7 on implementing appropriate ISO standards. They can be a major aid in establishing an effective IT security environment.

Second, in almost any IT operations there is a need to establish effective IT perimeter security. While the locked computer operations center from the mainframe days is less of a risk today, security risks are much greater in Internet-based e-commerce environments. We will discuss some IT perimeter security controls that should improve IT governance processes in these areas.

Third, we will discuss the importance of establishing an effective, enterprise-wide security strategy. Just as an employee code of conduct sets some high-level rules for all enterprise stakeholders, an effective IT security strategy establishes some IT security–related rules. A well-designed and well-implemented IT security strategy can improve many aspects of enterprise operations. IT management should be aware of effective best or good practices in these areas and should use these to establish an effective IT security environment.

ENTERPRISE IT SECURITY PRINCIPLES: GENERALLY ACCEPTED SECURITY STANDARDS

Through their own work, their contacts with enterprise financial managers, or their external auditors, many senior managers are aware of what are called generally accepted accounting principles (GAAP). While today GAAP is being replaced with international accounting standards, these are the informal rules that financial managers and their

external auditors use to assess enterprise accounting practices and then prepare enterprise financial statements. They are not point-by-point specific rules but a set of general good practices that external auditors have used over the years.

With an approach similar to GAAP, many enterprise IT management functions have implemented generally accepted system security principles (GASSP) as a set of best practices for developing effective IT security processes and standards. GASSP is a consensus set of IT security–related principles, standards, conventions, and mechanisms that IT security practitioners should employ, that information processing products should provide, and that information owners should acknowledge to ensure the security of their information and IT systems. GASSP relates to physical, technical, and administrative information security and encompasses pervasive, broad functional and detailed security principles. Its nomenclature defines a series rules, procedures, and practices that relate to the implementation of effective IT security practices in an enterprise. With ongoing rapid changes in IT technology, GASSP is expected to evolve accordingly.

GASSP's origins go back to 1990 when the U.S. National Research Council published the landmark book, *Computers at Risk* (CAR),[1] which emphasized the urgent need for the United States to better focus attention on information security. GASSP is a direct result of a key recommendation from that CAR report that called for the development of a comprehensive set of generally accepted system security principles that would provide a clear definition of IT security's essential features, assurances, and practices. The CAR report proposed using GAAP as a model for GASSP and also cited building codes and standards by Underwriters Laboratories[2] as examples of GASSP in other fields.

Another leading IT security professional organization, the International Information Systems Security Certification Consortium (ISC)[2], has since developed GASSP, with its current version 2.0 released in 1999.[3] As its name implies, these principles are generally accepted; that is, they represent concepts commonly being used at the present time to secure IT resources. The principles in that GASSP study are not new to the IT security professional, but are based on the premise that (almost) everyone should apply them when developing or maintaining an IT security system. The enterprise manager, seeking to promote security as part of effective IT governance, should be aware of GASSP as a standard for promoting effective IT security.

GASSP

GASSP is based on eight high-level principles that management and IT security specialists can use as an anchor on which to build their IT security programs. These principles are intended to be a security guide when creating new systems, practices, or policies. They are not designed to produce specific answers, and should be applied as a whole, pragmatically and reasonably. Each of the eight GASSP principles is expressed and explained as follows:

1. **IT security should support the mission of the enterprise.** The purpose of IT security is to protect an enterprise's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the enterprise's mission by protecting its physical and

financial resources, reputation, legal position, employees, and other tangible and intangible assets. Unfortunately, security is sometimes viewed as thwarting the mission of an enterprise by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. As a result, IT management should be aware that well-chosen security rules and procedures do not exist for their own sake—they are put in place to protect important assets and support the overall organizational mission.

Security, therefore, is a means to an end and not an end in itself. For example, an enterprise's security practices are usually secondary to its need to make a profit. Security, then, *ought to* increase the firm's ability to make a profit. In a public-sector agency, security is usually secondary to that agency's providing services to citizens. Security, then, *ought to* help improve these public services. Thus managers and security specialists need to understand both their overall enterprise mission and how each IT system supports that mission. After these system roles have been defined, these security requirements can then be explicitly stated in terms of the enterprise's mission.

2. **IT security is an integral element of sound management practices.** IT systems are often critical assets that support the mission of an enterprise. Protecting these assets can be as important as protecting other resources, such as money, physical assets, or employees. However, including security considerations in the management of information and IT systems does not completely eliminate the possibility that these assets will be harmed. Ultimately, management must decide what level of risk it is willing to accept, taking into account the cost of security controls.

   As with other resources, the management of information and IT systems may transcend organizational boundaries. When an enterprise's information and IT systems are linked with external systems, management's responsibilities extend beyond the enterprise, and both management and IT audit should know what general levels or types of security are employed on those external systems and should seek assurances that the external system provides adequate security for their enterprise's needs.
3. **IT security should be cost-effective.** An important IT governance principle, the costs and benefits of IT security should be carefully examined *in both monetary and nonmonetary terms* to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm. Requirements for security vary, depending on the particular IT system.

   IT security should be viewed as a smart business practice, and by appropriately investing in security measures an enterprise can reduce the frequency and severity of IT security-related losses. For example, an enterprise may estimate that it is experiencing significant losses per year in inventory through the fraudulent manipulation of its IT inventory control system. Security measures, such as an improved access control system, may significantly reduce this loss. Moreover, a sound security program can thwart hackers and reduce the frequency of viruses.

   Security benefits have both direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control

software or facility fire suppression systems. Additionally, security measures can sometimes affect system performance, employee morale, or even retraining requirements. All of these should be considered in addition to the basic cost of an IT security control itself. In many cases, such as in the costs of administering an access control package, these additional costs may well exceed the initial cost of the control. Solutions to security problems should not be chosen if they cost more, in monetary or nonmonetary terms, directly or indirectly, than simply tolerating the problem.

4. **Systems owners have security responsibilities outside of their own organization.** If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of security measures so that other users can be *confident* that their system is adequately secure. This does not imply that all systems must meet any minimum level of security but does imply that system owners should inform their clients or users about the nature of the security.

   The difference between responsibility and accountability for IT security is not always clear. In general, *responsibility* is a broader term, defining obligations and expected behaviors. The term implies a proactive stance on the part of the responsible party and a causal relationship between the responsible party and a given outcome. The term *accountability* generally refers to the ability to hold people responsible for their actions. Therefore, people could be responsible for their actions but may not be held accountable. For example, an anonymous user on a system is responsible for behaving according to accepted norms but cannot be held accountable if a compromise occurs since the security violation action cannot be traced to an individual.

   This principle implicitly states that people and organizations have a shared responsibility and accountability for their IT systems. In addition to sharing information about security, enterprise managers should act in a timely, coordinated manner to prevent and respond to breaches of security to help prevent damage to others. However, taking such action should *not* jeopardize the security of systems.

5. **IT security responsibilities and accountabilities should be made explicit.** The security-related responsibility and accountability of owners, providers, and users of IT systems and other parties concerned with IT systems security should be explicit. These responsibilities either may be internal to an enterprise or may extend across enterprise boundaries. Even a smaller enterprise should prepare documentation that states an enterprise's security policies and explicit IT security responsibilities. However, this element does *not* mean that individual accountabilities must be provided for on all systems. For example, many information dissemination systems do not require user identification or employ other technical means of user identification and therefore cannot hold users accountable.

6. **IT security requires a comprehensive and integrated approach.** Providing effective IT security requires a comprehensive approach that considers a variety of areas both within and outside of the IT security field and extending throughout the entire information systems life cycle. To work effectively, security controls often depend on the proper functioning of other controls. Many such interdependencies exist. If appropriately chosen, managerial, operational, and technical controls can

work together synergistically. However, without a firm understanding of the interdependencies of security controls, they can actually undermine one another. For example, without proper training on how and when to use a virus-detection software package, users may apply the package incorrectly and therefore ineffectively. As a result, users may mistakenly believe that if their system has been checked once, it will always be virus-free and may inadvertently spread a virus. In reality, these interdependencies are usually more complicated and difficult to ascertain.

The effectiveness of security controls also depends on such factors as systems management, legal issues, quality assurance, and internal and management controls. IT security also needs to work with traditional enterprise security functions including physical and personnel security. Many other important interdependencies exist that are often unique to the enterprise or system environment. Managers should recognize how IT security relates to other areas of systems and enterprise management.

7. **IT security should be periodically reassessed.** IT systems and the environments in which they operate are dynamic. System technology and users, data and information in the system, risks associated with the system, and security requirements are ever-changing. Many types of changes affect system security, including technological developments, changes in the value or use of information, and the emergence of a new threat. In addition, security is untested and *never* perfect when a system is implemented, and system users and operators frequently discover new ways to intentionally or unintentionally bypass or subvert security. Changes in an IT system or its environment can create new vulnerabilities. Strict adherence to security procedures is rare, and procedures become outdated over time, making it necessary to periodically reassess IT systems security.
8. **IT security is constrained by societal factors.** The ability of IT security to support the mission of an enterprise may be limited by such factors as social issues where security and workplace privacy can be in conflict. For example, IT system security is often implemented by identifying users and tracking their actions. However, expectations of privacy vary and can be violated by some security measures. Although privacy is an extremely important societal issue, it is not the only one. The flow of information, especially between a government and its citizens, is another situation where security may need to be modified to support a societal goal. In addition, some authentication measures may be considered invasive in some environments and cultures.

Security measures should be selected and implemented with the recognition of the rights and legitimate interests of others. This may involve balancing the security needs of information owners and users with societal goals. However, rules and expectations change with regard to the appropriate use of security controls. These changes may either increase or decrease security. The relationship between security and societal norms is not necessarily antagonistic. Security can enhance the access and flow of data and information by providing more accurate and reliable information and greater availability of systems. Security can also increase the privacy afforded to an individual or help achieve other goals set by society.

Implementing Security Principles in the IT Organization

While the eight GASSPs are not definitive, they outline a general framework that should be the basis for many aspects of good IT security and governance. Moving beyond them, an enterprise IT security function should rethink and reorganize some practices in order to embrace GASSP. Exhibit 10.1 shows the role of high-level security principles, such as GASSP, in an enterprise with consideration given to its installed technology products and other factors. While there are many ways to implement these security principles, IT management should not lose track that GASSP is based on some broad and strong IT security principles. These pervasive principles address the properties of IT security information confidentiality, integrity, and availability. They provide general governance guidance to establish and maintain the security of information.

We will go around the points in Exhibit 10.1 to briefly describe some of the key elements of GASSP and how they relate to one another and to an overall IT security environment. Each of these areas may differ, based on the enterprise, its size, and its domicile. We start at the center of Exhibit 10.1 with the security standards and other mechanisms, move up to the body of knowledge, and then clockwise around to the other factors necessary to form an effective security environment using GASSP:

- **Security standards and mechanisms.** The core of any effective security environment is a set of strong enterprise-specific security standards, mechanisms, practices, and conventions. These are the types of issues that have been discussed throughout these chapters as effective IT governance general control processes.

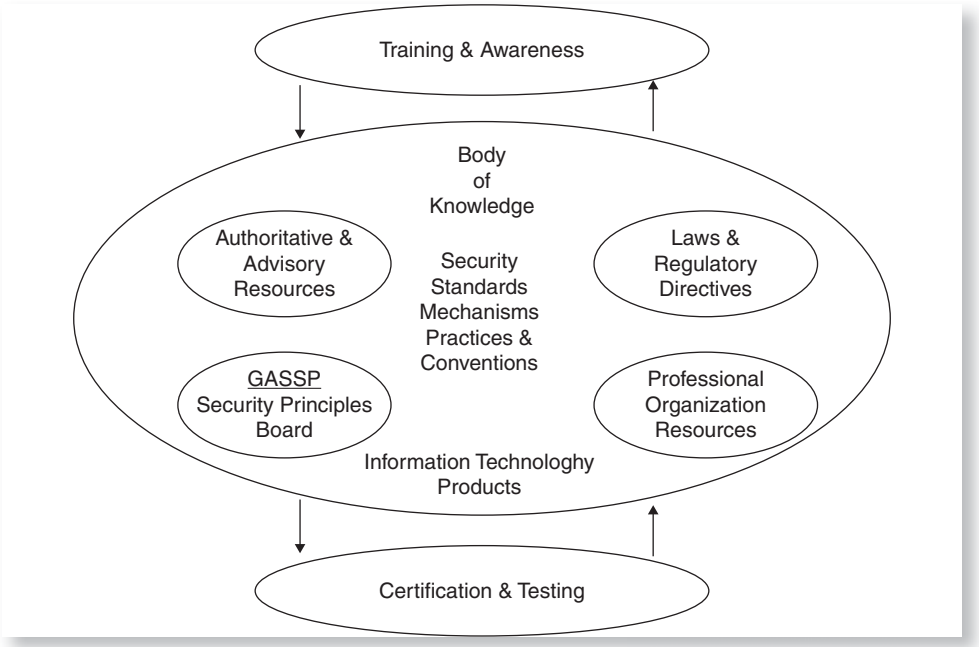

EXHIBIT 10.1 Role of High-Level IT Security Principles in the Enterprise

- **GASSP body of knowledge.** We have summarized GASSP's principles here, but a wide variety of persons in an enterprise should understand these broad principles and have expressed a commitment to understand and implement them on a regular basis. The idea is that if there is a question about some IT security practice, enterprise IT management should go back to these broad principles to help interpret and resolve any issues.
- **Laws and regulatory directives.** Every enterprise is subject to a variety and often differing set of laws and regulations. A good example here can be found in personal privacy laws that differ greatly from one country to another. GASSP must always be interpreted based on these different and sometimes often-changing rules.
- **Professional organization resources.** Professional organizations such as ISACA or the AICPA regularly issue guidelines and standards that add new requirements to IT security approaches or change approaches. An enterprise must be aware of these matters and make changes to its IT security environment accordingly.
- **IT infrastructure and security products.** There is a wide variety of IT application and infrastructure products that may help direct or modify approaches to IT security. While an enterprise should not install products that are deficient in these security principles, it is always necessary to be aware of any unique characteristics of such installed products and to make appropriate adjustment to other IT security practices.
- **GASSP security principles board.** When an enterprise embraces GASSP, it needs to install some authoritative persons to properly interpret its applications of GASSP. Someone from the IT security function, the quality assurance group, or a representative from a function such as IT internal audit may be an appropriate resource here. While no one may be an "expert" on GASSP, the idea is to appoint a responsible person who understands GASSP principles, can interpret them based on any questions raised, and can be an umpire or referee when needed.
- **Authoritative and advisory resources.** Although it does not typically sell consulting services, an enterprise should be closely tied with professional organizations such as ISACA or $(ISC)^2$ for any updates and other interpretive materials about GASSP.
- **Training and awareness.** GASSP is of little value to an enterprise unless key stakeholders are trained on its principles. System developers, in particular, should be aware of the GASSP principles and use them when launching secure, effective applications for the enterprise.
- **Certification and testing.** There are no GASSP certifications or testing programs in place at present, but such programs may be developed in the future.

Although GASSP has not received a wide level of acceptance by enterprises in the United States to date, with our ever-changing and technologically advancing world today as well as ever-growing IT security concerns, GASSP provides an important basis or framework for looking at and assessing IT security. Senior managers looking for ways to establish effective IT security and governance procedures might look to GASSP as a starting point.

IMPORTANCE OF AN EFFECTIVE, ENTERPRISE-WIDE SECURITY STRATEGY

There can be considerable value to embracing and implementing a set of broad security principles, such as GASSP, but an enterprise also needs to embrace and implement an overall IT security strategy. Security in today's IT-centric and electronic world involves complex architectures and continually emerging and evolving technologies. To ensure that an enterprise has established appropriate levels of IT security, it should consider using a top-down security model to identify and evaluate its security assets. Using such a top-down security approach, management can better understand the seriousness of IT security issues and can then initiate processes that are percolated down to operations staff. This differs from a bottom-up approach, in which the less-senior operational staff initiates the process and then propagates their findings upward to management as proposed policy recommendations.

Exhibit 10.2 is a simple illustration that shows this top-down security model concept, and the paragraphs following will discuss its elements in greater detail. An IT security infrastructure should apply equally to preexisting connections and to new initiative connections, and an organization's network should be protected based on the risk it represents to the enterprise.

The top level of the Exhibit 10.2 model calls for effective security policies. Although it sometimes seems almost too obvious, a senior manager reviewing controls in an IT security environment should initially develop an understanding of existing IT security policies for an enterprise. Although usually only at a high level, any such set of policies should cover all aspects of IT security. It may be sufficient to state that the enterprise's IT security polices will be based on the principles of the ISO standards discussed in Chapter 7, as well as COBIT from Chapter 5.

These strategies should be supported by detailed security standards that cover performing system monitoring, configuring a system as an application or Web server, or configuring a firewall to segregate systems into designated zones. The standards should be application- and operating system–specific, and detailed enough to enable a knowledgeable user to perform the activities highlighted in a standard or configure the system or application. Finally, the standards should specify the steps to be taken, such as sign-off, if a breach of these standards is required.

We should think of IT security operations in terms of a series of trust zones. That is, IT operations should identify and classify all current connections and systems into logical security-related zones. A key element of this security classification is access to the

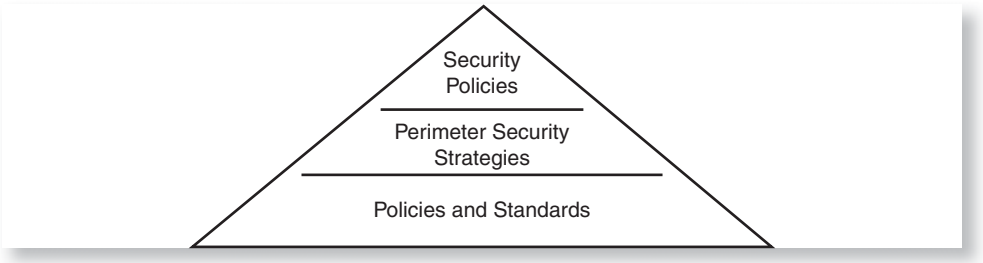

EXHIBIT 10.2 Top-Down IT Security Model Concept

Internet and other network connections such as vendor support systems. The following are four potential classifications for such interconnected systems:

1. **Trusted systems and processes.** These are systems directly under the control of the IT organization. Trusted users and systems potentially require full access to essentially all IT internal systems.
2. **Semi-trusted systems.** These are often vendor support and some business partner systems that require authenticated access to protect exposed systems that are not publicly accessible.
3. **Untrusted systems.** These are often customer-related systems and processes that require authenticated access rights to specific information resources, as well as exposed systems that are publicly accessible.
4. **Hostile systems and process threats.** Very restricted access rights should be allowed for these types of systems, and unauthorized access attempts should be detectable in real time.

Following these classifications, all levels of IT connections such as support vendors, customers, subsidiaries, and business partners should be reviewed and allocated to a level of trust based on the types of controls that can be maintained. However, identifying each connection in a large organization can be difficult at best. An effective method to launch such a classification is to conduct a workshop with a broad range of knowledgeable staff members who understand the associated concepts and are familiar with other projects within the enterprise and its IT operations. Although it is unlikely that a single workshop will identify all connections, this type of an exercise may help to identify the majority of connections and other staff members within an enterprise who may be responsible for identifying these and other connections.

These connections and their network connections protocols should be documented and used to develop detailed controls to allow accesses to and from appropriate destinations. As a result, the enterprise should segregate different parts of its network into multiple trust zones.

The segregation and classification of systems and processes provides for the separation of systems based on the defined trust categories. An enterprise's internal IT network always should have its own network segment, including Web, mail, domain name, and other servers that should be classified into trust zones and partitioned or segmented appropriately. This may result in each of these services being segmented on separate zones or may result in a number of these services being implemented into a single zone. The final design of perimeter security architecture will be dependent on the classification of systems and services, but the design of these security zones and classifications is a critical component of IT perimeter security.

IT CONTINUITY PLANNING

Over the years and particularly in the centralized mainframe computer days of old, enterprise IT auditors often raised issues regarding the risks of an enterprise losing a

substantial part of its IT resources due to some disastrous event. This was a particular concern in those early days of IT when most systems operations were based on centralized systems, there were few telecommunications connections to link IT resources, and those old mainframe systems were almost all vendor-installed custom installations where considerable efforts were necessary to install a new system.

Senior management recognized these system failure risks, and in response to these concerns, IT functions developed alternative processing strategies. This developed into the discipline that became known as IT disaster recovery planning, where an enterprise would often make arrangements for an alternative processing site to cover the risk of a mainframe's system failure. Since implementation of these plans could be expensive, IT audit and other managers often had a hard sell in alerting senior management to these risks. This author recalls leading an IT audit of disaster recovery planning for a then-major U.S. corporation in the early 1990s where one of its major data centers was located very close to a high-traffic airport—with the risk of an airline incident—and where no effective recovery plan was in place. When internal audit concerns about the lack of an effective IT recovery plan were first raised, the chief information officer (CIO) shrugged it off, saying such a disaster could "never happen." In the end, IT audit and this author had to raise these concerns in a meeting with the audit committee to get the corporation to launch such a disaster planning effort.

During the 1980s and early 1990s, a common IT disaster recovery solution for larger enterprises was to make arrangements with a remote disaster recovery data processing facility to handle emergency processing. Key backup files and programs were stored at off-site locations, with plans calling for the IT staff to shift to that alternative facility in the event of a disaster event. Professionals thought of IT disasters just in terms of fires, floods, or some other bad-weather situation. In those earlier legacy mainframe systems days, enterprises sometimes even utilized what today sound like bizarre methods for developing their IT disaster recovery plans. These included signing "reciprocal agreements" with nearby locations having similar IT resources so that each could move to the other's location for processing in the event of an emergency at either. Reciprocal agreements between two CIOs sounded good in theory, but they never really worked beyond low-level, basically humanitarian help. That nearby reciprocal agreement site might be out of service for the same weather-related disaster or probably would not be interested in someone else running their systems in off-shift time periods. As a final impediment, corporate legal counsel would have a dozen reasons to say no to a reciprocal agreement.

In those days, mainframe computer systems were housed in raised-floor facilities with space for cables and other gear in the floor and most mainframe computer systems were almost custom configured by a limited number of vendors (IBM, Amdahl, Univac, and a few others); a move to a replacement system in the event of an emergency was a challenge. In fact, doing this is much easier today, as computer hardware is usually off the shelf rather than custom manufactured and configured, as was common in the past.

Those early disaster recovery plans often were not very sound, but a series of specialized disaster recovery vendors soon appeared with fully equipped computer systems sites operating at idle (or what was called a "hot" site) to serve as an emergency backup

facility. In those days of centralized IT facilities, enterprises often contracted to use those "hot" sites as their disaster recovery facility, ran periodic tests, and kept key backup files there. Those old disaster recovery plans have gone away, and an IT organization needs to rethink its strategies here.

With our era of client–server storage virtualization and Web-based applications, an enterprise faces a new set of risks around its IT assets. There typically is not one central computer facility for handling major automated applications but rather a wide range of desktop devices, servers, cloud facilities, and other systems connected through often very complex communications, storage management networks, and links to the Internet. Enterprises do not have all of their IT resources tied around one central data center (or several), and management is more interested in keeping its IT facilities up and running than in worrying about the risk of losing a central computer systems facility. The original concept of IT disaster recovery planning was based on having processes in place to resume operations if some single disaster made the computer center inoperable. That earlier disaster recovery approach is not true today, but an enterprise needs to plan for business process continuity when faced with unexpected events.

With today's server and Internet-based systems, the language and strategic approaches to IT business continuity and disaster recovery planning have changed. Professionals should now think in terms of the importance of a business continuity plan (BCP), which consists of the procedures and processes necessary to restore overall business operations. The new approach and need is a BCP, rather than the disaster recovery plan of the past. The user of an online order processing system cares less about whether the server is operating than whether a customer order, submitted through an Internet site, can be processed properly and efficiently. The application should be restored and operating as quickly and efficiently as possible, but the key objective is to support and restore the business processes.

THE BUSINESS CONTINUITY PLAN AND IT GOVERNANCE

Some IT managers still think of risk and recovery in terms of a traditional disaster recovery plan, even though such plans were based on the old mainframe days long before the Internet. In IT's earlier days, there was a major emphasis on disaster recovery planning—the recovery of IT computer hardware systems, applications, and data files—but little attention was given to recovering basic business processes. While IT disaster recovery continues to be important, effective IT recovery procedures are often of limited value in today's world of interconnected Internet and now cloud-based systems. To support its IT governance processes, an enterprise should establish and implement a strong overall business continuity plan (BCP) covering the recovery of both its systems and its business processes.

For some professionals, this terminology presents ambiguities. A Web search for either "IT disaster recovery" or "continuity planning" brings up mixed references for both concepts, ignoring what we feel are significant differences between these two areas. Most of these references, despite their name, focus on traditional IT disaster recovery planning rather than more general BCP processes. As an example of this ambiguity, the

professional organization once called the Disaster Recovery Institute is now known as "DRI, the Institute for Contingency Management."[4]

No matter the size of operations or the criticality of its IT resources, every enterprise should have an effective BCP in place. With its emphasis on people, physical facilities, and other resources, the launch of an effective BCP requires the participation of a broad spectrum of enterprise mangers and others. However, because IT resources are a key BCP component, enterprise management should understand and play a key role in embedding a BCP in an enterprise.

An effective BCP extends beyond IT and involves the recovery, resumption, and maintenance of the entire business operations. While the restoration of IT systems and electronic data is important, recovery of these systems and data will not always be enough to restore business operations. There are many aspects to business continuity, such as a response plan for an unexpected flood in a mineral extraction mining operation. However, the discussion in this chapter covers business operations with extensive supporting IT operations.

An enterprise BCP involves the prioritization of business objectives and the critical operations that are essential for recovery. The processes should be structured in an enterprise-wide framework that considers every critical process, business unit, department, and system that will need to respond to disruptions and recovery solutions that should be implemented. This framework should include a plan for short- and long-term recovery operations. Without enterprise-wide BCP processes that consider all critical elements of the business, an enterprise may not be able to resume customer service and other operations at an acceptable level. Also, although it is often lacking in many enterprises today, management should prioritize their business objectives and critical operations that are essential for survival of the institution given that the restoration of all business units may not be feasible because of cost, logistics, and other unforeseen circumstances.

An effective BCP should include regular updates to that plan based on changes in business processes, audit recommendations, and lessons learned from testing. Changes in business processes include technological advancements that allow faster and more efficient processing, thereby reducing acceptable business process recovery periods. In response to competitive and customer demands, many enterprises today are moving toward shorter recovery periods and designing technology recovery solutions into business processes. These technological advances underscore the importance of maintaining a current enterprise-wide BCP.

However, because there can be so many variations in an enterprise's business operations and because of the many variations of what an enterprise needs to do to achieve continuity in the event of some unexpected event or catastrophe, it is difficult to prescribe BCP standards in any level of detail. To implement a BCP, enterprise management should consider the business continuity guidelines that have been developed by various professional organizations such as the U.S. National Fire Protection Association (NFPA), by computer vendors such as Oracle and HP, and by several national standards organizations. Perhaps the best and most recognized business continuity best practice materials have been released by the British Standards Institution (at www.bsi.gove.uk) and its related Business Continuity Institute, which publishes good practice guidelines.

These standards are similar to the ISO standards discussed in Chapter 7. Exhibit 10.3 is an overview of the BS 25999 life-cycle process.

We have described this BCP approach as a circular, continuous life-cycle process with the center or core of that process called BCP program management. As a first step for launching an effective BCP, a responsible manager in the enterprise should be made responsible for defining and managing the BCP program. Historically, enterprises looked to their IT function and assumed they would manage these BCP operations because of their responsibility for the IT disaster recovery plan, file backups, and periodic tests of that plan. However, there are often other continuity concern operations and functions that go beyond just IT, and others in the enterprise may be more appropriate parties to take responsibility for an enterprise-wide program.

For enterprises with an established a risk management function, the chief risk officer is usually the appropriate person to take the BCP program responsibility. In other situations, the chief information officer (CIO) can assume overall responsibility here or the task can be given to the enterprise's quality assurance function. The BCP is a very important element of enterprise IT governance, and in all cases the audit committee should review and approve this BCP strategy.

In addition, an enterprise needs to establish a high-level policy to define the scope and objectives of its BCP plans. It is easy for a senior manager to state that an enterprise's BCP will cover "everything," but high-level scope restrictions are needed. Even though such statements may sound impressive, there may be certain products or services that do not need to be included in any top tier of the BCP plans.

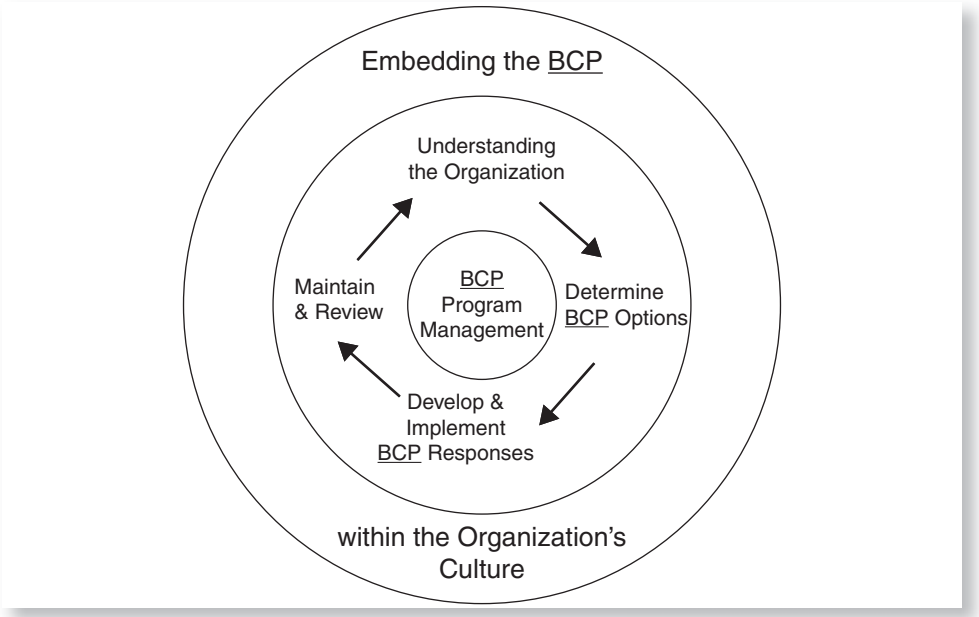

EXHIBIT 10.3 Business Continuity Plan (BCP) Life Cycle

Under the leadership of the enterprise function given responsibility for its BCP, a team should be established to develop a business continuity policy for the enterprise. This can include:

- Reviewing any existing enterprise continuity planning materials, such as existing IT disaster recovery plans or weather emergency plans, to determine the appropriateness of their BCP procedures.
- Identifying any good practice guidelines, regulations, or legislation that must be included in any BCM plan.
- Performing a high-level BCP risk assessment, that is, identifying all key systems, product lines, business units, or other functions that require the highest business continuity priorities.
- Developing an enterprise business continuity policy and discussing its assumptions to obtain approval from senior management and the audit committee.
- Publishing the approved BCP policy as a high-level guide to launch the overall enterprise business continuity program.

The approved BCP should then become a basis for enterprise continuity planning activities. This is a core governance concept that will allow the enterprise to embed continuity planning into the overall enterprise culture. The business continuity guidance materials discussed in this chapter should use this as beginning step to launch an effective set of BCM processes. As discussed, we should soon see this template, or a very close pattern, become a worldwide standard for business continuity process just as the Committee of Sponsoring Organizations (COSO) internal control framework, discussed in Chapter 4, has become a worldwide standard.

The BCM life-cycle model shown in Exhibit 10.3 outlines processes for understanding the typical business organization. As a result, an enterprise should be in a position to choose appropriate continuity strategies to enable it to meet its BCP objectives. The enterprise should launch a suite of alternative operating processes to use after an interruption to maintain or resume business activities in each key area. Based on assessed risks, these strategies should depend on a range of factors such as the maximum tolerable period of disruption for some critical activity, the cost of implementing a strategy, and the consequences of any inaction.

A significant difference between following the BCP model and older, more traditional disaster recovery approaches is that planners should not think of just one continuity strategy for the enterprise but rather a stream of differing activity-level approaches for the enterprise. The complexity of interdependencies on services, business processes, data, and technologies needs to be analyzed, with appropriate tactics chosen to address the needs of:

- **People in the enterprise.** There is a need to identify appropriate strategies for maintaining the core skills and knowledge of people in the enterprise. Many of the needs here cover such areas as documented job descriptions, succession planning, and many of the other practices that should be promoted by a good human resources (HR) function. However, BCP strategies should always recognize that

key people may not be available for the resumption of an activity, and people-based continuity processes should always be in place.

- **Work site needs.** The enterprise should devise a strategy for reducing the impact of the unavailability of normal work sites. In most cases, this involves identifying alternative locations for continuing operations or even an employee working from home strategy for some activities. If some enterprise facilities are involved in such activities as heavy manufacturing or chemical processing, however, an alternative site might not be readily available, and other activity-level strategies may even include withdrawing from operations in the short term.
- **Supporting technologies.** Enterprises are dependent on their IT facilities, telecommunications network processors, product testing resources, and a wide range of other devices, depending on the product or industry. While many enterprises already have developed strong IT disaster recovery plans, an enterprise needs to gain a good understanding of its other technology-based activities to develop appropriate BCP strategies.
- **Physical and virtual Information.** In addition to IT resources and other technology-based tools, an enterprise should have a wide range of information-related activities that are represented in physical or hard copy as well as virtual or soft copy formats. Any information required to deliver critical activities should have appropriate confidentiality, integrity, availability, and currency controls.
- **Equipment and supplies.** The enterprise should identify and maintain an inventory of the core supplies and equipment that support critical activities. Activity-based strategies may include the storage of supplies at alternative locations, arrangements with third parties for delivery of supplies, holding certain supply materials in separate warehouses, or the identification of alternative supply sources. Where critical activities are dependent on specialist supplies, alternative suppliers should be identified or contractual arrangements should be made with existing key suppliers.
- **Stakeholders, partners, and contractors.** The enterprise should develop appropriate strategies to manage relationships with key stakeholders, business or service partners, and contractors. The BCM strategy should consider and protect the interests of these key stakeholders.

Developing a business continuity plan and a supporting strategy can really be a major effort covering all enterprise activities. The overall BCP should consider continuity threats in relation to the linkages and interconnections of all major enterprise activities. Because of the many interconnections in all types of business operations, there are few freestanding, totally independent activities.

Effective IT security practices are complex tasks requiring strong enterprise IT technical support. Similarly, business continuity planning requires the overall support of IT as well as senior management. However, both of these are important components of effective IT governance processes.

NOTES

1. *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Academies Press, 1990), http://www.nap.edu/openbook.php?isbn=0309043883.
2. Underwriters Laboratories (UL) is an independent, not-for-profit product-safety testing and certification organization. It has tested products for public safety for more than a century, www.ul.com/global/eng/pages.
3. Mariane Swanson and Barbara Guttman, Generally Accepted System Security Principles (GASSP), NIST, Version 2.0, June 1996, http://csrc.nist.gov/publications/PubsSPs.html.
4. Disaster Recovery Institute International, Falls Church, VA, www.drii.org.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER ELEVEN

PCI DSS Standards and Other IT Governance Rules

THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) is an information security best practice as well as an industry required standard for the many enterprises that handle cardholder information for the major debit, credit, automatic payment (ATM), and retail point-of-sale (POS) cards. Defined by the PCI Data Security Standards Council, PCI DSS was created to increase controls around cardholder data to reduce credit card fraud through a series of recommended best practices. With our worldwide reliance on payment cards for all forms of business, enterprises that accept credit cards for business operations at any level must comply with PCI DSS. An understanding of PCI DSS and its compliance requirements is an important element of IT governance for many senior business managers today.

This chapter will introduce PCI DSS and discuss its control objectives to help build and maintain a secure IT network. We will discuss the compliance requirements that fall under these rules, with both the processes for qualified security assessments for larger enterprises as well as the voluntary use of the PCI DSS Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes. PCI DSS rules cover much more than consumer credit card transactions, and compliance here is an important part of IT governance.

This chapter also briefly introduces two other U.S. laws that have an impact on IT governance: the Gramm-Leach-Bliley Act (GLBA) covering the collection, disclosure, and protection of consumers' nonpublic personal information, and a discussion of the IT recordkeeping rules that are elements of the health-care act known as HIPAA. Our discussion of the GLBA and HIPAA are examples of the many laws and rules that we encounter today that include IT governance issues.

In the United States, the European Union, and elsewhere in the world, these and a seemingly endless number of other new laws, rules, and standards have been issued that include at least some IT governance issues. In addition to this chapter's information

on PCI DSS, GLBA, and HIPAA, other chapters cover different IT governance rules and standards. For example, Chapter 7 introduced ISO international standards for IT governance, and Chapter 17 will discuss IT service level agreements and the ISACA Val IT guidance, both very important for IT governance. The enterprise IT executive should always be at least aware of these and other new laws, rules, and standards and their impact on good IT governance practices.

PCI DSS BACKGROUND AND STANDARDS

Starting in the early 1960s, embossed plastic "credit cards" became common tools initially for business and professional consumers to buy airline tickets, pay for business dinners, and buy gasoline. Some of the early general card issuers, such as American Express, are still with us, while other credit card brands, with names such as Carte Blanche and Diners Club, have gone away. Other cards were issued for just a brand of gasoline or for a store and were good only for those products or merchants. The American Express type of card was particularly popular because it could be used at a variety of merchants who would agree to accept it, but it remained a somewhat elite credit card, with strong personal credit standards over card issuance.

Visa and MasterCard credit cards were created in the 1970s, and Discover came along in the early 1980s. Each of these was authorized and issued by a cardholder's local bank with a separate group managing the card brand and card usage fees for businesses accepting the cards. The usage of these credit cards has boomed, with many consumers today carrying a pocketful of cards all issued by different banks.

Credit cards have prospered worldwide, but there have been growing levels of credit card fraud, security, and protection risks. While a bank is responsible for issuing credit cards to individuals, separate management companies have been formed for each major card brand. For example, one handles all Visa cards, and there is another for MasterCard. Regarding card security, each card management company's intentions have been roughly similar: to create an additional level of protection for card issuers by ensuring that their merchants meet minimum levels of security when they store, process, and transmit cardholder data.

To better resolve small differences that have existed between different credit card brands, the Payment Card Industry (PCI) council was formed. Security issues and differing rules were a major problem among all PCI members, and in 2004 these credit card companies aligned their individual policies and formed a Security Standards Council that released the first version of their PCI DSS. This is a standard and not a law, but merchants using cards are expected to act in compliance.

Given all of the changes in credit card processing in recent years with such features as wireless processing, the risk of the theft of otherwise legitimate credit card numbers stored in enterprise business records, and other increased risks of fraud, PCI DSS has gone through multiple revisions since its first release. Compliance with PCI DSS standards is achieved through voluntary self-assessments for smaller PCI users, while compliance is mandatory for larger credit card processors. Whether an IT professional or any business operation using payment cards today, business executives

should have at least a general understanding of PCI DSS and its impact on business operations.

Exhibit 11.1 outlines the PCI DSS high-level requirements and associated control objectives. The sections following will discuss the intent of PCI DSS requirements in greater detail, outline requirements for maintaining cardholder data, and then discuss the nature and importance of the PCI DSS self-assessment processes. Other chapters discuss matters that are important for effective PCI DSS compliance. For example, Chapter 10 discussed IT security issues that are important for effective IT governance. These same issues are equally important in achieving PCI DSS compliance.

In addition to the DSS, the PCI has issued two related standards:

1. **PCI PTS.** A set of security requirements focused on the management of devices used in the protection of cardholder personal identification numbers (PINs) and

EXHIBIT 11.1 PCI DSS Requirements and Associated Control Objectives

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data acrosss open, public networks.
Maintain a Vulnerability Management Program	5. Use and regularly update antivirus software on all systems commonly affected by malware. 6. Develop and maintain secure systems applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that assesses information security.

other payment processing–related activities, including requirements for the design, manufacture, and transport of a device to the entity that implements it.

2. **PA DSS.** This standard is for software developers and integrators of payment applications that store, process, or transmit cardholder data as part of the authorization or settlement when these applications are sold, distributed, or licensed to third parties.

Although these other two standards are related, our discussion in this chapter will focus on PCI DSS, a standard important to IT governance in many enterprises.

Protecting Cardholder Data and Vulnerability Management Programs

It is fairly easy for a small merchant to make banking arrangements with Visa, MasterCard, or others and then install readers or scanners to accept these cards as payments for purchases. This card purchase information is transmitted to the credit card processor, the merchant receives payment for the purchased goods, and the purchaser is billed on a credit card statement. There is one major and often ignored security risk in this very common process. The credit card number along with other customer identifying data may be stolen and used for improper purposes. For example, in one incident, a reported more than 100 million personally identifiable customer records were breached in the United States over the two years ending in 2007.[1] Improper use of such breached credit card numbers presents risks for the merchant, the credit card company, and the card owner. A major objective of PCI DSS is the requirement to protect this stored cardholder data. One can expect that a provider such as Visa, MasterCard, and its affiliated banks will have secure systems—banking regulations require such—and an individual is expected to protect his or her own individual credit card data. However, merchants typically handle and process many customer credit card numbers over time. A major PCI DSS requirement is that an enterprise should secure and protect that credit card data.

A problem here is that merchants often inadequately secure too much of their customer credit card data. As part of a major 2007 study of merchants in the United States and the European Union, the consulting firm Forrester[2] found that merchants typically keep too much of their customers' credit card data, including the card numbers, expiration dates, customer names, and addresses. Enterprises typically store much more than just the credit card number, including expiration dates, names and addresses, and security codes. Lacking strong enterprise IT security measures, this poorly secured credit card information creates a security exposure for many.

Encryption and other security controls are often weak or not even implemented, and enterprises processing a high volume of transactions sometimes may face risks due to their lax handling of customer credit card materials. An example of the risks and exposures can be seen through events in 2003 at TJX Companies, the owner of about 2,500 retail stores. TJX computer systems were first breached by a hacker who accessed information from credit card customer transactions over multiple months until discovered in 2006.[3] Information, including customer names and credit card numbers, from 45.7 million credit and debit cards was stolen from

transactions between January and November of that year. The credit card privacy of many customers was lost, and TJX faced huge losses in litigation settlements and reputation.

The TJX event is an example of the risks an enterprise can face if their credit card–related controls are weak. A postmortem analysis of such a security breach will typically show common security weaknesses that are now addressed by PCI DSS. A special type of IT security control, PCI DSS is designed and includes detailed requirements for exactly this type of risk—to minimize the chance of compromise and the effects if a compromise does occur. Investigations after compromises consistently show common PCI DSS violations, including but not limited to:

- Inadequate access controls due to improperly installed merchant POS systems, allowing malicious users to access paths intended for POS vendors.
- Lack of logging or monitoring via such techniques as log reviews, intrusion detection/prevention, quarterly vulnerability scans, and file integrity monitoring systems.
- Storage of credit card magnetic strip data. Many compromised entities are unaware that their systems are storing this data, which provides vast information to an intruder.
- Default system settings and passwords that were not changed when a system was set up and unnecessary and insecure services that were not removed or secured when a system was set up.
- Poorly coded Web applications resulting in vulnerabilities that allow access to the database storing cardholder data directly from the Web site.
- Poorly implemented network application controls, resulting in the cardholder data environment being unknowingly exposed to weaknesses in other parts of the network that have not been secured, such as unsecured wireless access points and vulnerabilities introduced via employee e-mail and Web browsing.

Our objective is not to provide a tutorial on IT security issues but to emphasize that IT security is an important element of IT governance and that it is especially critical for credit card–related transactions. The senior manager can use the above points to ask questions about the security and integrity of an enterprise's credit card operations. However, since most credit card information is transmitted directly from the POS terminal where the sale is transacted to the credit card processes, a basic rule of thumb for a merchant is to never internally transmit this customer credit card data.

PCI DSS Requirements

With the combined efforts of its IT, internal audit, legal, credit, and finance staffs, an enterprise should take the necessary steps to establish PCI DSS compliance, as summarized in Exhibit 11.1. PCI DSS has the following general requirements:

- **Build and maintain a secure network.** Chapter 10 talks about the importance of IT security in an enterprise, but the PCI DSS standards have two specific

requirements here. First, an enterprise should build, install, and maintain firewall configurations on its IT systems to protect cardholder data. The concept of a firewall is common for IT security professionals but may not be familiar to the business executive. We can think of an IT firewall as similar to the one-way exit doors found in most theaters. One can go through these doors to the outside in case of a fire, but someone from the outside cannot enter them. While firewall controls are common today for many IT security environments, enterprises should assure that they have been installed for those elements of their IT systems covering credit card data.

In addition, an enterprise should not use vendor-supplied defaults for system passwords and other vendor-defined security parameters. This is a simple security good practice that is often ignored. A software vendor may instruct new customers to enter "1234" as a starting password when first setting up an application and then to change it once installed. All too often application user personnel do not bother to change that default password and the system remains vulnerable for an intruder to gain access.

- **Protect cardholder data.** There are many IT security controls in this requirement, including backing up data for retrieval if needed, encrypting the data in storage and transmissions, and storing any cardholder IT media in physically secure locations. Processes to protect that cardholder data are an important IT governance requirement.
- **Maintain a vulnerability management program.** Chapter 8 talked about IT risk management, and there should be a particular emphasis on the use of risk management and vulnerability assessment techniques for credit card data stored or processed through an enterprise site. Also, the enterprise IT function should use and regularly update antivirus software to predict against malware.
- **Implement strong access control measures.** Strong IT security processes are needed to fulfill this requirement. Some key control techniques are to:
  - Restrict physical access to cardholder data.
  - Restrict access to cardholder data by business need-to-know.
  - Assign a unique ID to each person with computer access.

  These are some key IT access controls, and business executives can ask their IT security staff to provide them with a detailed briefing on enterprise IT access control techniques. Although there are many published and Web-based sources for information on IT security and access control, this author has developed a book[4] on these topics that is oriented to IT auditors but also can provide the business executive with some good IT security background briefings.
- **Regularly monitor and test networks.** An enterprise should track and monitor all access to network resources and cardholder data. In addition to monitoring and tracking, PCI DSS includes a requirement to regularly test its security systems and processes. This will often be the responsibility of internal audit and their IT auditor specialists. Internal audit IT governance issues are discussed in Chapter 19.

- **Maintain an information security policy.** This final PCI DSS policy calls for an enterprise to maintain policies that address information security. This is very similar to other IT governance processes discussed over these many chapters. It is one thing for an enterprise to recognize best practices that need to be implemented, but these should be communicated to all involved stakeholders as general rules that must be followed.

The above actual PCI DSS requirements are much more specific than the general guidance discussed in this section. The more senior enterprise manager will look for high-level standards, while the IT computer security specialist will seek more detailed requirements. For example, Exhibit 11.2 contains DSS guidance for one of these requirements. These standards are at the level of a skilled IT auditor or IT security specialist. The point here is that an enterprise must establish some strong control procedures in order to remain PCI DSS compliant.

For the medium- to larger-size enterprise that has had experience with building and operating its own IT systems over time, the PCI DSS requirements may seem little more than the good internal control practices that have been common and are basic requirements to achieve Sarbanes-Oxley compliance, as discussed in Chapter 2. A fundamental difference, however, is that an enterprise will not be subject to an external audit to attest to its level of PCI DSS compliance. Rather, industry standards here call for most enterprises with lesser amounts of credit card activity to go through their own self-audit or assessment process to review and then establish PCI DSS compliance.

EXHIBIT 11.2 Requirements for Tracking and Monitoring Access to Network Resources and Cardholder Data

1. Establish a process for linking all access to system components to each individual user—especially access done with administrative privileges.
2. Implement automated audit trails for all system components for reconstructing these events:
   - All individual user accesses to cardholder data.
   - All actions taken by any individual with root or administrative privileges.
   - Access to all audit trails.
   - Invalid logical access attempts.
   - Use of identification and authentication mechanisms.
   - Initialization of the audit logs.
   - Creation and deletion of system-level objects.
3. Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component, or resource.
4. Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time.
5. Secure audit trails so they cannot be altered.
6. Review logs for all system components related to security functions at least daily.
7. Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.

The PCI DSS Self-Assessment Process

In order for an enterprise to assert that it is in compliance with or is following some standards requirement, it is normally necessary to rely on some outside party to confirm that compliance. For example, external auditors—CPA firms in the United States—are necessary to review and attest that an enterprise's financial statements are fairly stated. Similarly, specialized independent reviewers are necessary to help an enterprise assert that it is in compliance with any of the ISO standards, including those discussed in Chapter 7. Since there are so many—often relatively small—merchants handling customer credit card data and the cost of bringing in external reviewers would be almost prohibitive, the PCI standards organization allows for an enterprise self-assessment review.

The PCI DSS Self-Assessment Questionnaire (SAQ) is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with PCI DSS standards. Detailed multiple copies of these standards can be found at www.pcisecuritystandards.org/security_standards/index.php. These self-assessment standards call for the following:

- Based on the PCI guidance "Selecting the SAQ and Attestation that Best Apply to Your Organization," an enterprise should select an SAQ appropriate for its service providers and merchants.
- After successfully completing an appropriate SAQ, an enterprise can attest its self-certification that it is eligible to perform and has actually performed a PCI DSS self-assessment.

Industry standards require that all major users of credit cards must hire an independent assessor to review that compliance, similar to the ISO compliance reviews discussed in Chapter 7. Even for smaller enterprises, compliance with data security standards can bring major benefits to the busines, while failure to comply can have serious and long-term negative consequences. PCI DSS compliance is important because:

- Compliance with the PCI DSS means that systems are secure and customers can trust an enterprise with their sensitive payment card information.
- Compliance improves one's reputation with acquirers and payment brands—the partners you need in order to do business.

Compliance is an ongoing process, and it should not be a onetime event. It helps prevent current and future security breaches and the theft of payment card data. As data compromise becomes ever more sophisticated, however, the PCI Security Standards Council is regularly working to monitor threats and improve the industry's means of dealing with them, through enhancements to PCI security standards and by the training of security professionals.

Compliance has indirect benefits as well, which may help an enterprise to be better prepared to comply with other regulations, such as HIPAA, discussed later in this chapter, and SOx, introduced in Chapter 2. In other words, this self-assessment can

provide a basis for a corporate security strategy and may identify ways to improve the efficiency of the IT infrastructure.

GRAMM-LEACH-BLILEY ACT IT GOVERNANCE RULES

In the late 1990s, the U.S. Congress passed legislation to change some of the financial institution rules that had been in place since the Great Depression of the 1930s. This new law is officially known as the Financial Modernization Act of 1999, better known as the Gramm-Leach-Bliley Act (GLBA). GLBA is a privacy-related set of requirements with the objective of protecting individual consumers' personal financial information held by financial institutions. This privacy-related legislation has three principal parts: (1) the Financial Privacy Rule, (2) the Safeguards Rule, and (3) what is called its "pretexting provisions." While certainly most professionals have never heard of what the GLBA calls "pretexting," that concept and its IT governance considerations from other sections of this regulation will be discussed in the following sections. GLBA gives authority to eight different U.S. federal agencies and the states to administer it, and it enforces a new set of privacy-release rules that apply to what are generally called "financial institutions." These institutions include not only traditional banks, securities firms, and insurance companies but also enterprises providing many other types of financial products and services to consumers. Among these are the lending, brokering, or servicing of any type of consumer loans, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, residential real estate settlement services, collecting consumer debts, and an array of other activities. With GLBA, these nontraditional "financial institutions" are now regulated by the Federal Trade Commission (FTC) either directly or through other federal and state agencies.

While a senior manager working for a bank or insurance company today probably has been involved with these 1999 GLBA and its privacy-related provisions, the act is a rule that may impact many other enterprises due to its expanded definition of what are called "financial institutions." GLBA rules are also being applied to many state-regulated financial institutions. As an example, insurance companies in the United States are regulated on a state-by-state basis, with the National Association of Insurance Commissioners (NAIC) acting as a central coordinating and standards-setting group for these state-chartered insurance commissions. The NAIC has imposed the federally mandated GLBA rules on its individual state-regulated insurance companies. This is another example of how U.S. federal regulations move in some instances from a U.S. authority like the Securities and Exchange Commission (SEC), for SOx matters, to rules covering state laws as well as even some similar international financial rules. We often forget that in the United States some corporate regulations and many other legislative rules are effective on a state-by-state basis. For example, motor vehicle driver's licenses are issued by each of the states. Similarly, although the certified public accountant (CPA) examination is administered nationally by the American Institute of Certified Public Accountants (AICPA), CPAs are licensed on an individual state basis through individual state boards of accountancy. Through the authority of the NAIC, a state rule coordinating body, GLBA rules are being adopted by most of the states in the United States.

GLBA Financial Privacy Rules

U.S. consumers frequently encounter the GLBA and its Financial Privacy Rule today when they receive an often innocuous note from a credit card provider describing the privacy rules for that credit card. The GLBA Financial Privacy Rule requires financial institutions to give their customers these privacy notices that explain the financial institution's information collection and sharing practices. This privacy notice must be a clear, conspicuous, and accurate statement of the company's privacy practices; it should include what information the company collects about its consumers and customers, with whom it shares this consumer credit information, and how it protects or safeguards the information. The notice applies to the "nonpublic personal information" the company gathers and discloses about its consumers and customers; in practice, that may be most—or all—of the information an enterprise has about its customers. For example, nonpublic personal information could include the information that a consumer or customer puts on a credit or sales contract application; information about the individual from another source, such as a credit bureau; or information about transactions between the individual and the company, such as an account balance. Indeed, even the fact that an individual is listed as a consumer or customer of a particular financial institution is classified under GLBA as nonpublic personal information. Matters that the company has reason to believe are lawfully public—such as mortgage loan information in a jurisdiction where that information is publicly recorded—are not restricted by GLBA.

GLBA-mandated privacy notices must contain the following information elements:

- The types of nonpublic personal information an enterprise collects regarding its customers;
- The types of nonpublic personal information the enterprise will disclose to others about the customer;
- The parties to whom the enterprise discloses this information, other than under an exception to the prohibition on nondisclosure;
- The customer's or client's right to "opt out" of the disclosure along with simple rules for opting out;
- Enterprise policies with respect to sharing information about a person who is no longer a customer or client; and
- Enterprise practices for protecting the confidentiality and security of the customer's or client's nonpublic personal information.

Many consumers today pay little attention to these notices even though they may state that the company that has their account data may share the consumer's name with others. Rather than the all-too-common consumer practice of crumpling and tossing this note, GLBA gives the customer the right to opt out of (say *no* to) having this consumer private information shared with certain third parties. The privacy notice must explain—and offer in a reasonable way—how they can opt out. For example, providing a toll-free telephone number or a detachable form with a preprinted address is a reasonable way for consumers or customers to opt out, but requiring someone to write a letter as the only way to opt out is not. The privacy notice must also explain

that consumers have a right to say no to the sharing of certain information, such as credit report or application information, with the financial institution's separate divisions or affiliates.

GLBA puts some limits on how anyone who receives nonpublic personal information from a financial institution can use or redisclose the information. If a lender discloses customer information to a service provider responsible for mailing account statements, where the consumer has no right to opt out, that service provider may use the information for only limited purposes—such as for mailing account statements—and may not sell the information or use it for marketing.

This GLBA Financial Privacy Rule gets more complex as we get into its details. Our intention here, however, is not to give such a detailed explanation of this portion of GLBA but to explain these privacy rules and the IT governance impacts in general. Enterprise managers should recognize that all personal financial information is very private and cannot just be just arbitrarily sold or otherwise distributed. Consumers have rights to opt out and say no, and the enterprise must keep appropriate records of these actions and respect consumer privacy rights. The same is true for any enterprise that has a consumer-related credit-granting and billing facility. A risk to an enterprise is that it may take the GLBA Privacy Rule as an almost trivial matter, perhaps failing to honor an opt-out request, or improperly selling a mailing list, and then finding itself facing some type of class action litigation for damages due to the failure to comply.

GLBA Safeguards Rule

GLBA Safeguards Rule requires financial institutions to have a security plan in place to protect the confidentiality and integrity of personal consumer information. When consumers open an account or purchase some product, they will often disclose some element of their personal information—such as an address, telephone number, or credit card number—as part of that application transaction process. An enterprise must have a security plan in place to protect the confidentiality and integrity of that consumer-supplied personal data. It should cover more than just the business continuity risks briefly discussed in Chapter 10 and include controls to prevent hackers from accessing data files, disgruntled employees accessing customer information, or just simple carelessness. The GLBA Safeguards Rule requires that every financial institution, regardless of size, must create and implement a written information security plan for the protection of customer data. The scope and complexity of this security plan may be scaled to the size of the institution and the sensitivity of the information it maintains. The plan should be based on a risk analysis that identifies all foreseeable threats to the security, confidentiality, and integrity of customer information. Based on that risk analysis, financial institutions must document and implement security measures that include administrative measures such as employee training; technical protections, including passwords, encryption controls, and firewalls; and physical safeguards such as locks on doors and computers. Financial institutions must designate one or more of their employees to coordinate these safeguards, and must conduct periodic reviews to determine whether their security programs require updating in light of changed circumstances.

An enterprise can demonstrate compliance with the GLBA Safeguards Rule through the following steps:

1. **Environmental risk analysis.** The enterprise should formally identify the internal and external risks to the security, confidentiality, and integrity of all customer personal information. Risk analysis approaches were discussed in Chapter 8. This process should cover the risks or loss or disclosure for all sources of personal information, whether on automated systems or manual records.
2. **Designing and implementing safeguards.** These safeguards are essentially the internal control procedures discussed in Chapter 4 as part of the Committee of Sponsoring Organizations (COSO) internal control framework.
3. **Monitoring and auditing.** Continuous audit assurance monitoring processes should be in place, and senior management should encourage its internal auditors to regularly schedule reviews of the adequacy of an enterprise's security plan, coupled with appropriate compliance tests.
4. **Constant improvements program.** As a result of any weaknesses reported through audits or other tests, an enterprise should have a program in place to constantly improve its security plan. That program should be well documented and describe the plan's progress.
5. **Overseeing security providers and partners.** Many partners and other enterprises may have access to this same personal information or may just have access to systems network connections where that personal privacy can potentially be violated. Adequate policies, controls, and audit procedures need to be in place here as well.

The GLBA Safeguards Rule applies to a wide range of providers of financial products and services, including mortgage brokers, nonbank lenders, appraisers, credit reporting agencies, professional tax preparers, as well as retailers that issue their own credit cards. Banks are not subject to the Safeguards Rule, but must comply with similar counterpart regulations that have been issued by federal banking agencies. Failure to comply with the Safeguards Rule may result in fines or other enforcement action by the FTC.

GLBA Pretexting Rules

Using an expression that will signal errors in the spell-checkers of word-processing programs, GLBA prohibits "pretexting," the use of false pretenses, including fraudulent statements and impersonation, to obtain consumers' personal financial information, such as bank balances. Pretexters use a variety of tactics to get personal information. For example, a pretexter may call, claiming she is from a survey firm, ask a few questions to perhaps get the name of one's bank, and then use the information gathered to call the target person's financial institution, pretending to be that targeted person or someone with authorized access to that account. She might claim that she has forgotten her checkbook and needs information about the account. In this way, the pretexter may be able to obtain personal information about the target victim such as a Social Security number, bank and credit card account numbers, information in

someone's credit report, or the existence and size of personal savings and investment portfolios.

Under GLBA's Pretexting Provisions, it is illegal for anyone to:

- Use false, fictitious, or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Ask another person to get someone else's customer information using false, fictitious, or fraudulent statements or using false, fictitious, or fraudulent documents or forged, counterfeit, lost, or stolen documents.

Pretexting leads to a new security and privacy risk or exposure—"identity theft." This occurs when someone hijacks your personal identifying information to open new charge accounts, order merchandise, or borrow money. Consumers targeted by identity thieves usually do not know they have been victimized until the hijackers fail to pay the bills or repay the loans and collection agencies begin dunning targeted consumers for payment of accounts they did not even know they had. According to the FTC, the most common forms of identity theft are:

- **Credit card fraud.** A credit card account is opened in a consumer's name or an existing credit card account is "taken over."
- **Communications services fraud.** The identity thief opens telephone, cellular, or other utility services in the consumer's name.
- **Bank fraud.** A checking or savings account is opened in the consumer's name, and/or fraudulent checks are written.
- **Fraudulent loans.** The identity thief gets a loan, such as a car loan, in the consumer's name.

A separate federal law, related to GLBA, the Identity Theft and Assumption Deterrence Act, makes it a federal crime when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law." Here, a name or Social Security number is considered a "means of identification," as is a credit card number, cellular telephone electronic serial number, or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual.

GLBA is one of the rules that can impact many senior managers, particularly those working in any type of financial institution. While many aspects of GLBA are primarily designed to protect consumer financial information, that definition has become so broad that GLBA potentially impacts a wide range of enterprises in the United States. Financial and credit-granting enterprises should become more aware of these GLBA rules as well as their general privacy rules that are applicable for many other enterprises. The Web is

the most appropriate source to obtain additional more detailed and current information on GLBA and its provisions. Two good sources are:

1. **Federal Trade Commission.** This government source provides an overview of GLBA as well as its most current rules at http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.
2. **National Association of Insurance Commissioners.** This state-by-state regulatory enterprise has general GLBA information at www.naic.org as well as several other Web sites covering detailed related subjects.

Although GLBA continues to be an important item of U.S. legislation, it has almost been placed in the background since 2011 with the complex requirements of what is called Dodd-Frank. The Dodd-Frank Act implements changes that, among other things, affect the oversight and supervision of financial institutions, provide new resolution procedures for large financial companies, create a new agency responsible for implementing and enforcing compliance with consumer financial laws, introduce more stringent regulatory capital requirements, effect significant changes in the regulation of what are called counter-derivatives, reform the regulation of credit rating agencies, implement changes to corporate governance and executive compensation practices, require registration of advisers to certain private funds, and effect significant changes in the securitization market. In other words, it does a lot!

It is a complex item of legislation, its rules just being drafted as this book went to press. From our limited review of the legislation, it appears to have few direct IT governance concerns. However, it is another item of legislation that creates new rules for many enterprises today.

HIPAA: HEALTH CARE AND MUCH MORE

A U.S.-based manager today who is visiting a doctor for an annual physical or some other procedure will be asked to sign what looks like an innocuous disclosure permission agreement before getting started when checking in at the front desk. These permission documents ask the patient to agree to allow his or her medical records to potentially be shared or disclosed as part of that visit. If the enterprise manager patient asks why, the response will usually be that this is a "legal requirement of HIPAA." The medical patient's typical reaction is to sign the document and move on, not fully understanding this signature request. Although a health-care-related set of rules, HIPAA contains a set of privacy-related legislative rules that go beyond health care and will impact many enterprises and their internal auditors.

Whether working for a U.S. manufacturing company, a financial services enterprise, or many others, senior managers need to have at least a general understanding of some of the Health Insurance Portability and Accountability Act (HIPAA) rules. Enacted in 1999 with the final rules released over subsequent years, HIPAA has had a major impact in the United States on the privacy and security of personal medical records as well as many other personal records. Individuals encounter HIPAA when visiting a

doctor's office or for many other medical-related matters. Human resources functions in enterprises are also seeing the impact of HIPAA requirements today in their administration of employee health-care plans and medical treatment records. Of course, HIPAA has caused a large and ever-growing impact on the entire health-care industry and all affiliated delivery providers. Even more significantly, HIPAA rules cover a wide range of electronic commerce–based business processes.

The original HIPAA legislation has four primary objectives:

1. Assuring health portability by eliminating preexisting-condition job locks. This was the original motivation that led to the passage of HIPAA. People were diagnosed with some condition and then often were unable to acquire new health coverage when changing employers because information about that health condition was often cavalierly shared with others.
2. Reducing health-care fraud and abuse. These words are from the congressional hearings leading to the legislation when some examples of alleged fraud and abuse were cited.
3. Enforcing standards for health information. This is covered by the HIPAA privacy and security rules outlined next.
4. Guaranteeing the security and privacy of health information.

This section will provide a brief overview of HIPAA objectives and its resultant rules covering IT governance, privacy, and security. While not an exhaustive introduction to all aspects of HIPAA, we have introduced it as another of the legislatively driven "new rules" that continue to impact many enterprise senior managers. The progress of the HIPAA legislation also illustrates how the government-sponsored rule-making process often works. HIPAA rules were initially issued in draft form following an early published schedule. The drafts resulted in lots of comments, revised rules drafts were issued with still more comments, and the final rules were issued much later than originally planned.

HIPAA Patient Record Privacy Rules

Ongoing concerns regarding medical patient privacy were the motivating reasons for the U.S. Congress originally passing HIPAA. We visit a medical care provider, discuss some concern or problem, and then expect treatment in a manner that is confidential or private. We do not want the results of that medical office or physician visit to be communicated back to our employer's human resources department, or to some other insurance company that has no need to know, or to be left on a desk in the medical care provider's office for anyone to pick up. Even worse, we do not want any personal, confidential matters to be shared in a manner that may limit our future employment options. This personal information privacy concern is the basis for much of HIPAA. However, many parties need to have some information about our health-care condition to provide adequate coverage or reimbursement, and virtually all health-care operations require detailed and complex supporting systems. HIPAA privacy rules cover five general areas, briefly outlined in the paragraphs following. These comments do not provide an exhaustive coverage of and are not intended to be a reference source for HIPAA rules;

they are intended to provide the nonmedical professional with an overview of these HIPAA new rules:

1. **Medical records uses and disclosures.** An enterprise that is subject to HIPAA rules must take steps to limit the use and disclosure of personal medical information to "the minimum necessary to accomplish the intended purpose of the use, disclosure, or request" for non-treatment-related matters. We start this overview of HIPAA rules by directly quoting some of the words contained in these rules. Using expressions such as "the minimum necessary," the act contains many such guidelines that will be subject to enterprise-specific practices that are to be validated through other rulings or litigation over time.

   This section of HIPAA rules goes on to specify that an individual's health information loses its HIPAA protection if the individual covered is "de-identified" in a manner that this health information will not contain any of 18 specific identifiers of the individual and his or her relatives, employers, or household members. This requirement says a lot about HIPAA. In order to make a health-related information system HIPAA compliant, the legislation identifies these 18 specific factors that an IT specialist in database retrieval might use to identify an individual. That is, an individual's medical information that is placed in some type of file or information system is generally protected from general disclosure to others, but that information can be shared if it meets certain specific conditions.
2. **Authorization requirements.** This is the section of HIPAA that many users of health-care services first encounter. Health-care providers must obtain written approval to disclose health-care information on everything except emergency situations. An individual has the right to refuse such a disclosure and health-care providers have a strong record retention requirement to keep track of all of these disclosures. These are the documents, as previously discussed, that an individual is asked to sign when visiting a physician's office.
3. **Privacy practice communications.** Health-care providers must have published privacy practices that they should provide to health-care users. Individuals then have the right to formally request restrictions in this policy, and providers must accommodate reasonable requests.
4. **Medical record access and amendment rights.** Individuals have the right to inspect and copy all or a portion of their personal health information. In addition, individuals have the right to request amendments to those health-care records. Finally, the health-care provider must keep a record of all other parties that requested access to these personal health-care records in the six-month period prior to any request.
5. **HIPAA privacy administration.** Going beyond the records access and disclosure rules, HIPAA has an extensive set of privacy administrative requirements. These rules apply to what are called "covered entities"—medical offices, laboratories, hospitals, and all others involved with personal health care. These privacy administration rules include:

   - The provider must designate a "Privacy Official" who is responsible for the development and implementation of these HIPAA policies and procedures.

- The provider must train members of its workforce on these HIPAA privacy-related policies and procedures and must maintain documentation to demonstrate that the training has been provided.
- A health-care provider must have in place administrative, technical, and physical safeguards to protect the privacy of personal health information.
- The health-care provider must apply "appropriate sanctions" against employees who fail to comply with these privacy policies and procedures.
- The provider must develop and implement policies and procedures that are designed to comply with the elements of the HIPAA regulations, and this documentation must be maintained in written or electronic form for six years.

While these HIPAA rules primarily cover access to personal health-care information, they outline other areas that define good operating practices that should be implemented elsewhere in the enterprise. An example would be the requirement that health-care providers maintain documentation covering their training programs. These types of rules have existed for Federal Drug Administration medical or drug programs, are now part of HIPAA, and are a good idea for most corporate training programs. Enterprises sometimes spend resources in training their employees but often do not bother to document that activity very well.

These rules and others in this chapter are particularly important to an enterprise executive working in a health-care-related enterprise, such as a hospital or medical claims insurance company. However, the rules extend to other areas as well, such as medical insurance claims processing in an enterprise's human resources department or factory floor safety and industrial accident reporting. Health-care-related enterprises should have strong HIPAA compliance rules and procedures, but it is beyond the scope of this book to provide a detailed description of these rules. However, HIPAA compliance is required in many other environments as well. Exhibit 11.3 describes some HIPAA IT governance procedures that should be in place in any enterprise subject to HIPAA.

Cryptography and HIPAA Security Requirements

In addition to its medical records authorization and release privacy rules, HIPAA contains some very specific and, for many smaller enterprises, difficult-to-implement IT security requirements. It pushes to the edges of IT security practices for many and requires such things as secure electronic signatures even though there currently are limited technically mature techniques to provide such security on open networks such as the Internet. We are still at a point where a skilled computer hacker can intercept a cell phone call, and such a call covering health-care-related matters could create a violation of HIPAA security requirements. Technology will change in the future, control procedures will improve, the hackers will get ever smarter, and violations will be settled in the courts.

The basic reason behind these security rules was that many pre-HIPAA health-care IT administrative systems were inadequate. Enterprises can often improve this system's security not merely by purchasing and installing new software but by first improving human-driven policies. HIPAA security standards rules were finalized and

EXHIBIT 11.3 HIPAA IT Governance Requirements and Procedures

1. The enterprise should be defined as a health-care-related enterprise and subject to HIPAA. (If not, no need to complete steps.)
2. An enterprise-wide information security officer should be appointed for HIPAA compliance as well as a general HIPAA implementation plan developed.
3. Policies and procedures to protect patient health information should be developed and implemented.
4. Processes should be in place for the ongoing support and monitoring of HIPAA rules and regulations.
5. HIPAA processes should include comprehensive privacy and security policies, procedures, controls, and technologies.
6. An enterprise should have a formal contingency plan in place that includes:
   - Application and data criticality analysis.
   - Data backup planning.
   - Disaster recovery plans.
   - Emergency mode operations plan.
   - Periodic testing and revisions to the plan.
7. HIPAA processes should include formal information access control processes, including access authorization, access establishment rules, and access modification procedures.
8. Controls over access to information systems media should include processes for:
   - Accountability.
   - Data backup.
   - Data storage.
   - Disposal of data.
9. Personnel security policy/procedures should:
   - Ensure the supervision of maintenance personnel by an authorized, knowledgeable person.
   - Maintain a complete record of access authorizations.
   - Ensure that operating and maintenance personnel have proper access authorization.
   - Provide for a personnel clearance procedure.
10. Formal termination procedures should be in place, including the changing of appropriate combination locks and the removal from access lists.
11. Physical access controls throughout the facility should include:
    - Emergency mode operation plans.
    - Equipment control into and out of facility.
    - Facility security plans.
    - Procedures for verifying access authorizations prior to physical access.
    - Maintenance records.
    - Need-to-know procedures for personnel access.
    - Sign-in for visitors and escort, if appropriate.
    - Testing and revisions to the physical access plan.
12. All networks and communications should be protected through:
    - Automatic logoff.
    - Unique user identification.
    - Passwords and PINs.
    - Telephone callbacks.

put into effect until April 2003, but compliance standards for these rules did not take effect until 2006. Among other areas, these rules cover what HIPAA calls "covered entities" that include:

- Doctors and other health-care providers who process health-care claims electronically.
- Health plans, including enterprises that self-insure.
- Health-care clearinghouses—billing services and others who provide data formatting services for electronic claims submission.

This means that HIPAA security rules apply to all enterprises whether a single doctor's office, a major hospital, or a small professional office that handles its own health-care claims processing through self-insurance.

Security is a key HIPAA element for keeping personal health information private, and these rules cover good security practices for much more than just medical records, such as requirements for strong disaster recovery standards. The published rules consist of both "required" and what HIPAA calls "addressable" rules. The latter are rules that an enterprise is not required to implement due its small size and limited resources. The "required" HIPAA rules represent many good information security practices that are appropriate to any enterprise. Other HIPAA security areas here are beyond the scope of this book, such as requirements for a public key infrastructure environment that includes digital signatures.

HIPAA IT Security Administrative Procedures

HIPAA requires administrative procedures to be in place to guard data integrity, confidentiality, and availability. These procedures must be carefully documented per HIPAA rules, and Exhibit 11.4 lists some of these "required" administrative procedures. Also listed in Exhibit 11.4 are implementation rules in a very general manner, but the published HIPAA rules tend to be very detailed. Many of these requirements, such as a documented and tested contingency plan or formal policies for information access controls, are similar to the control procedures internal auditors have been recommending over the years. Some of these represent good IT governance practices that should be in place in many enterprises. For example, provision number 3 in Exhibit 11.4 refers to the need for what is called a sanctions policy—a formal set of rules for people who violate security policy. This is a good idea for most enterprises! Now, as an administrative rule, a HIPAA-impacted health-care provider will face a penalty if its established rules and procedures are found inadequate.

HIPAA security requirements also include physical safeguard rules that are similar to the physical access controls that have existed over IT data centers going back to the early days of mainframe computers. Here, however, HIPAA goes beyond the classic IT operations center and calls for strong guidelines and documentation over workstation use and location. While IT management and its internal auditors typically have not raised that many internal control concerns regarding the physical controls for networked terminals in a business facility environment, the HIPAA-regulated health-care

EXHIBIT 11.4 HIPAA Required Implementation Specifications

Provisions for "covered" entities as part of a HIPAA security and compliance plan.

1. Risk Analysis. Enterprises must conduct a thorough assessment of the potential risks of information confidentiality, integrity, and availability.
2. Risk Management. Covered enterprises must implement reasonable and appropriate security measures to reduce overall risks to an acceptable level.
3. Sanctions Policy. Sanctions or related penalties must be applied to workforce members who violate the enterprise's security policy, such as a "three strikes and you're out" type of policy.
4. Information Systems Security Activity Reporting. Security logs, incident reports, and related security activity reports should be reported and reviewed on a regular basis.
5. Incident Response Procedures. Processes should be in place to identify, investigate, mitigate, and document security incidents.
6. Backup Procedures. Appropriate procedures must be in place to recover any loss of data.
7. Disaster Recovery. Every covered enterprise must establish procedures to cover any loss of data.
8. Emergency Mode of Operations. Processes must be in place to ensure the security of patient information when operating in an emergency mode.
9. Related Business Contracts. An enterprise must include language in supplier contracts that requires suppliers adopt adequate security measures to report security incidents to the enterprise, to ensure these subcontractors implement appropriate security measures, and to provide for the termination of the contract in case of a security breach.
10. Disposal of Patient Information. Policies and procedures should be in place to address and archive the final disposition of patient information.
11. Media Reuse. Processes must be in place to ensure the removal of sensitive information from electronic media, such as disk drives, before reuse.
12. Unique User Identification. Unique identifiers must be assigned to all systems users in order to prevent shared accounts and to track system behavior.
13. Emergency Access Procedures. Procedures must be established to allow for the accessing of electronic information during an emergency.
14. Documentation. Procedures must be established to guarantee information security, maintain the documentation for a period of six years, and review it periodically.

environment introduces new issues. A medical environment workstation that may be used by doctors, nurses, or other staff members requires strong logical and physical controls to protect the personal privacy of the patient records that may pass through those workstations.

Technical Security Services and Mechanisms

HIPAA rules require that processes should be put in place to guard the integrity, confidentiality, and availability of this medical records data and to prevent unauthorized access to any data that is transmitted over communications networks. The rules require IT systems security controls that are often stronger than those found in some larger corporations today and include:

- **Access controls.** Strong control mechanisms based on the context of the data or the role or position of authorized users must be established. In addition, control

processes must always be in place to allow emergency access from data center operations if required.

- **Audit controls.** Here and throughout all of the HIPAA rules are requirements for strong audit controls, including such things as documentation revision processes and traditional audit trails.
- **Data authentication.** Strong systems controls over data integrity are required here.
- **Entity authentication.** Controls must be in place such that when one workstation attempts to access another, it should be authenticated. This process may include passwords, telephone callbacks, or even biometric controls. This requirement goes beyond many enterprise practices in place today, where information is often freely shared through an e-mail note with attachments.
- **Communications and network controls.** A wide range of controls are suggested, including alarms, encryption, event reporting, message authentication, and others. The HIPAA-impacted enterprise must implement a very secure network.

HIPAA requires that electronic signature controls be established that will provide the same legal weight to electronic data signatures as is associated with a traditional signature on a paper document. HIPAA prescribes network message integrity, no repudiation, and user authentication for any message with an electronic signature. For many, this can be a challenge. Digital signature processes are in place today, but they are often somewhat cumbersome and will be required until other, better techniques are developed.

HIPAA rules have pushed progress in many areas of IT security and integrity. Although developed for health-care enterprises, these rules will impact many enterprises. Senior executives should try to stay generally aware of these ongoing rules and their required standards even if not working directly for a health-care enterprise. This chapter has provided a very limited introduction to these complex and important rules. Going beyond just a health-care enterprise, they apply whenever health-related records are maintained by a human resources function. An interested manager can find more HIPAA information from two important sources:

1. **U.S. Department of Health and Human Services.** Copies of HIPAA rules and other supporting reference materials are available from www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.
2. **HIPAA Advisories.** A site maintained by Phoenix Health Systems as a public service is a good source for HIPAA information at http://www.phoenixhealth.com.

HIPAA compliance is a U.S. legal requirement. While government auditors are not going to be visiting hospitals or large health-care facilities, and certainly not commercial organization human resources departments, an individual who feels there has been a violation can file a complaint with the U.S. Department of Justice (DOJ). That could certainly occur if some key information from an employee's medical insurance claim records became public knowledge due to a records security breakdown. The DOJ has a complaint-driven/voluntary compliance approach.

Interested senior managers should be aware of HIPAA rules and their related IT governance issues, at least on a high level. They are another strong reason for an enterprise to implement strong security and confidentiality controls over any area that might impact an employee's medical health records.

NOTES

1. Privacy Rights Clearinghouse (PRC), https://www.google.com/#hl=en&sclient=psy-ab&q=privacy+rights+clearinghouse&oq=Privacy+Rights+Clearinghouse+&gs_l=serp.1.3.0l3j0i30.0.0.1.9354.0.0.0.0.
2. "The State of PCI Compliance," Forrester Consulting, September 2007, www.rsa.com/solutions/PCI/ar/RSA_AR_State_of_PCI_Compliance.pdf.
3. Multiple accounts of TJX's troubles can be found, such as "T.J. Maxx Data Theft Worse Than First Reported," MSNBC.com, March 29, 2007, www.msnbc.msn.com/id/17853440/ns/technology_and_science-security/t/tj-maxx-data-theft-worse-first-reported/#.Tp2.
4. Robert Moeller, *IT Audit, Control, and Security* (Hoboken, NJ: John Wiley & Sons, 2010).

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER TWELVE

IT Service Catalogs: Realizing Greater Value from IT Operations

AS WE HAVE DISCUSSED IN PREVIOUS CHAPTERS, in the earlier days of IT systems, business users went to their IT department managers or systems personnel and requested that they upgrade their existing IT systems or launch new ones. Requests then were often for little more than new or different format paper-based reports. These users, however, often complained about poor IT service because their requested systems projects were delivered late, did not meet expectations, or had other problems. This was in the days when there were limited IT systems and services and certainly before the days of the Internet. The requesting users typically outlined their needs and completed some type of formal request for IT services. IT would review, often approve, and schedule the requested work—sometimes sooner but more often later than the desired user-initiated request.

IT services today are much more complex than just the regularly delivered financial and operational reports of years past. System users today often have needs for special analyses based on other existing systems; they may have some special procedure timing needs due to international legal reporting requirements, or they have an interest in some new technology they encountered at a trade show and are interested in seeing the same in their enterprise. IT functions usually have many systems and tools at their disposal, but members of user community departments are often not aware of what IT services are available through their enterprise IT organization. Similar to the menu we encounter when visiting a restaurant, an IT function can aid its user community by offering them a menu or catalog of the services they offer. Users of IT resources frequently benefit from access to an IT service catalog when requesting or scheduling an IT service.

An IT service catalog is a list of services that an enterprise IT function should consider providing to its employees, customers, or other stakeholders. Each described IT-related service within such a catalog typically includes:

- **A description of the service.** This would be a list of existing IT applications or processes that a user function might want. Such applications must fit into overall business operations and their other system requirements.
- **Time frames or service level agreements (SLAs) for fulfilling the service.** SLAs are two-way processing types of internal agreements or informal contracts between IT and users of IT. An important IT governance tool, they are discussed in more detail in Chapter 17. The idea here is that an IT service catalog describes when some service can be delivered and user department requirements to fulfill that service offering.
- **Who is entitled to request or view the service.** The catalog should specify, for example, that certain special analyses reports are available only to certain employee levels in finance departments. Similarly, some catalog offerings might specify that requesting users must be responsible for resolving errors or formally reviewing certain systems outputs.
- **IT service costs.** The idea that IT facilities are a "free" resource within an enterprise has long gone, and Chapter 17 provides some additional IT governance support for managing and understanding the costs and pricing. Nevertheless, an IT service catalog should outline some high-level guidance on the costs of catalog service offerings.
- **How to fulfill the IT service listed in the catalog.** There should be some information on timing and required approval levels, and other information necessary to initiate a requested service from the catalog.

While a service catalog is an important tool for IT functions, the same concept is also valuable for many non-IT and even human resources function–related offerings. For example, a service offering application can be used to register for or change employee human resources benefits, to change contributions or disbursements from employee credit union or savings accounts, or to acknowledge acceptance of an employee code of conduct.

Enterprise IT functions can effectively publish their service offerings through an organization Web site available to only authorized stakeholders. A user can then go to this Web site to search for a specific service, such as requesting a new laptop system, a change in benefits, or adding a new employee to a department. The service catalog site groups offerings by category and allows for searching (especially when hundreds or thousands of services are available). The user selects a desired service and sees the description and details. The user enters any pertinent information, such as contact information or service-specific questions, and submits the request for service. The request requires approval, and goes through routing, service level management, and other processes necessary to fulfill the request. The user may return to the site later to check on the status of a request, or to view overall metrics on how well the organization is performing the services it provides.

An IT service catalog is an important and valuable governance tool for many enterprises. This chapter looks at how to establish and implement an effective IT service catalog as well as some key controls necessary to improve related IT governance processes. Because IT management sets standards and controls what resources should be listed

as IT services on its catalog, and because that catalog outlines the options available to an enterprise IT user community, a well-organized and well-controlled service catalog can be an important element of effective IT governance.

IMPORTANCE OF IT SERVICE CATALOGS

Because of growing business unit demands for new IT services and higher service levels as well as ongoing cost pressures, many larger enterprise IT operations functions have launched some fundamental transformations and changes in emphasis over recent years. Chief information officers (CIOs) and other IT executives have recognized the need to better align their services with the needs of the business, improve internal customer satisfaction, and deploy standardized processes to achieve greater operational efficiency. This imperative to improve service quality—and demonstrate value to the business—has driven many IT functions to implement improved service processes, such as ITIL, discussed in Chapter 6, as well as other IT process methodologies. An IT service catalog is a major component in the need to improve IT customer service.

The ITIL framework is based on the concepts of IT service and customer care, and an IT service catalog is at the core of these fundamental concepts. Many IT groups have produced a service catalog as part of their ITIL service level management deployment. However, even if an enterprise has not yet fully adopted ITIL concepts, an enterprise service catalog can serve as a focal point for interactions between IT and the business as well as providing both an opportunity to improve IT customer service. An IT service catalog is an important IT governance tool, essential for providing the foundation for defining services and communicating with the business.

To be effective, an enterprise IT service catalog must be understood, embraced, and used by the business. IT service catalogs became a "hot" new concept a few years ago, but all too often, IT departments have invested countless hours in creating service catalog documentation in a static or fixed format that few customers have ever read or used. Ultimately, many of these static service catalogs are rarely seen or read by either end users or business decision makers—and thus they often have little to no impact.

In order to build an effective IT service catalog, IT as well as enterprise business unit managers should determine what services to "publish" to their end users via their service catalog. The business unit managers and IT analysts typically should determine the types of questions that may be asked by their catalog users, any approvals necessary for a request, and what other systems or processes are needed to fulfill the request. Once the service is defined and the fulfillment process organized, the IT function should build the requisite functionality into the service definition and then publish this to the service catalog.

Customer service is not a new word for IT operations. However, in the early days of IT systems and operations, the IT function often all but decided what and when to implement. IT's high costs and user dissatisfaction with poor service and systems that did not meet needs led to massive rethinking of an IT function's service to its users. The growth of personal computer systems and the Internet has changed these concepts over the years. Today, many IT functions and enterprise management are realizing

that they are essentially a customer service function, providing systems support and other IT facilities to all aspects of their enterprise organization. The IT service catalog has become a key feature for helping to build and support IT customer service. However, in order to ensure a successful and customer-focused IT service initiative, IT organizations should follow three guidelines for building and developing an IT service catalog:

1. **Recognize that the IT customer is king.** First and foremost, an IT service catalog should be created with an unwavering focus on internal customer needs. The most common mistake IT organizations make is to place too much emphasis on articulating their services from an IT perspective. The customers of IT usually do not want to review detailed service descriptions in "IT-speak"—they want to see services described in terms they can understand, written in nontechnical terminology, and addressing immediate concerns or needs.

   Successful IT service catalogs are defined from the customer in, rather than from the infrastructure out. For guidance, successful IT service catalogs should be built similar to the real-life online catalogs that customers use every day—like Amazon.com, Dell, and eBay.

   An IT service catalog should look like one of these Web-based consumer catalogs, with easy-to-understand descriptions and an intuitive storefront interface for browsing available service offerings. An effective IT service catalog also segments the customers who may access the catalog—whether end users or business unit executives—and provides different content based on function, roles, needs, locations, and entitlements. This customer-focused approach helps ensure that the IT service catalog is adopted by end users and provides the basis for a balanced, business-level discussion on service quality and cost trade-offs with business decision makers.
2. **Make the IT service catalog actionable.** It is important that an IT service catalog be more than just a static repository of information. Using our example of Web-based consumer catalogs, consumers viewing an online catalog at Amazon.com or Dell.com assume that if they see something they want, they can order it. Likewise, an IT service catalog for end users should be tied to service request processes—with a Web-based shopping cart interface enabling end users to order services and track fulfillment status online. Similarly, business unit executives should have their own unique view of their enterprise's IT service catalog that provides greater transparency into detailed IT budget items, consumption drivers, service levels, and the business impact of each service that IT provides.

   IT services matter to employees when they want to upgrade their laptop systems or when they need to increase the size limit on their e-mail inbox. IT matters to business executives when they are reviewing budgets or when they receive their IT bill. It is at these moments that the IT service catalog needs to be available and actionable.

   To ensure success, the service catalog should become the single access point that end users will turn to for all their IT service delivery needs, and should be readily available anytime business customers want to understand what IT does and how well it does it. What all of this means is that IT services should be viewed as almost a commodity by the IT function. Senior managers who have been involved with

IT functions from past years formerly completed some type of a "Request for IT Services" type of document when they needed a new report or IT process. Those requests from older days went to some type of steering committee who first reviewed the request, approved it, and then set implementation priorities. Many IT processes today do not need the custom systems and programming work from past days, but user needs can still be achieved from many of today's IT systems and processes.

3. **Enable the IT service catalog to become a system of record.** An actionable IT service catalog should serve as a "system of record" that enables an IT service organization to be managed like a business within a business. The IT service catalog can provide the vehicle to manage customer demand, map fulfillment processes for each service, ensure service level compliance, drive process efficiencies, and track costs.

   No service-oriented business can run effectively without such operational and financial data readily and easily available. By providing internal customers with a central point for requesting services, IT can leverage this data to more effectively control consumption. With standardized and well-documented services, IT teams can enforce repeatable and measurable service delivery processes that ultimately result in predictable and reliable service quality. This allows IT executives to have access to the necessary information for business-relevant and fact-based discussions with their business counterparts about budgets and pricing.

   An IT service catalog can be the cornerstone for success in many customer-focused IT initiatives. By defining and publishing a standard portfolio of business-relevant service offerings, an IT function can more effectively market its value and establish a framework for communication with the business. And by making the service catalog operational and transactional, IT operations can help standardize service fulfillment processes, manage consumption, and drive continuous improvement.

   Services that are not frequently requested can be discontinued. Delivery processes for high-volume services should be optimized. Key performance indicators can provide greater visibility to control costs, ensure optimal service quality, and support budgeting conversations with IT decision makers.

   With an actionable and customer-focused service catalog in place, an IT function can truly operate as a service-oriented provider that effectively meets the needs of its business customers. However, we must realize that an IT service catalog should not be offering the types of things found in the old-fashioned Sears Roebuck catalog of past times—with lots of diverse and even eye-popping entries. The service catalog should focus on important enterprise IT offerings.

ROLE OF A SERVICE CATALOG IN THE IT SERVICE PROVIDER ORGANIZATION

An IT service catalog should support business units that will use the catalog as well as the IT functions that supply IT services on strategic, tactical, and operational management levels. That is, such a catalog should first be built on a very high level where both senior management and CIO-level IT leadership can first decide on the types of offerings to be included in the catalog. For example, a financial trading enterprise may have a

need for a series of access tools to help it with its trading. Any individual investor who has looked at stock market selection software, for example, realizes that there are many, many stock selection and analysis tools. However, it is simply not feasible or economical to list all such analysis tools in an enterprise catalog available to any level of system user. Rather, both the business and IT need to screen these various alternatives and place only the ones that were accepted in the catalog.

Exhibit 12.1 shows this service catalog relationship between business units and the IT service provider organization. The triangle on the left does not necessarily represent the entire enterprise but may only be a separate division or operating group that has its own needs and systems. However, a specific IT systems and operations function would typically be supporting this independent business unit. The idea here is that the overall strategy for an IT service catalog should be established at a strategic level by senior IT management and senior operations and financial management. These create the top-level entries that form the basis for an IT service catalog and an enterprise service portfolio.

A strategic-level service catalog covers high-level IT service offerings, such as key features and options available from an enterprise resource planning (ERP) system that was implemented based on a software vendor selection and implementation project. Any ERP-level system provides many options and requires a high level of user and IT enterprise training and understanding to make use of such a system's features. ERP systems governance issues will be discussed in Chapter 15. The selected ERP type of a high-level system would be introduced into the service catalog at a strategic level.

A tactical management perspective is then necessary to build any service catalog and establish linkages between the IT function and its operations and business unit customer organizations. This is a multistep process described in Exhibit 12.2. As a first step, IT management should take a hard look at its existing IT resources and remodel them as

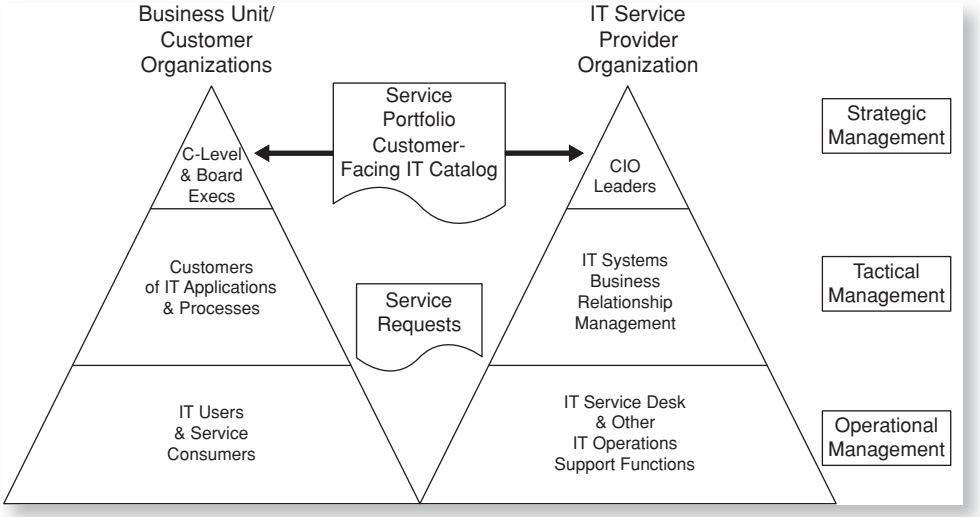

EXHIBIT 12.1 IT Service Catalog Business Relationships

specific user services. For example, an enterprise may have some major accounting and finance applications such as the month-end close general ledger. It may be necessary to highlight other special analyses processes here, describe them as well as identify their potential users, and establish them as entries into the service catalog. These will transition from just IT processes to customer-facing services, as described in Exhibit 12.2.

As a next step, the customer-facing IT services should move to specific business processes. This step forces the IT and business team to go beyond just a list of their implemented applications that can be described in a service catalog. The idea is to provide more details such that business processes can be better enabled. The IT catalog should better define these business processes to allow users to understand how to select and use business processes. An example of the type of process to add to such a catalog might be procedures for organization unit new hires. The typical organization unit is not bringing in very many new people on a regular basis, but there are special processes needed for such new personnel, including background checks, benefit and retirement plan offerings, code of conduct compliance, and many more. An IT catalog would drive users to these necessary services and steer them to achieve compliance.

AN IT SERVICE CATALOG'S CONTENT AND FEATURES

IT service catalogs are common offerings in many enterprises today. But they should be much more than just a long list of application file names similar to what can be found from a Windows-based operating system directory list. The types of services offered should be tailored to the organization and its objectives. A Web search of other enterprises can provide numerous examples of what an IT service data log should look like, although many Web resources describe vendor products marketing their own solutions. However, the typical service catalog begins as an Internet IT department home page for an enterprise that points authorized members of the enterprise user community to the IT available services.

While this author is not a professional in Web design, Exhibit 12.3 shows a front-facing or home page of a service catalog for the Global Computer Products example company referenced in other chapters. After logging in with an assigned user ID

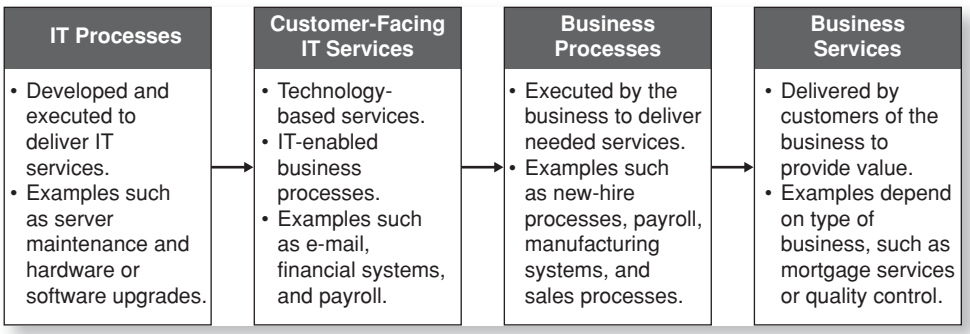
IT Processes
• Developed and executed to deliver IT services.
• Examples such as server maintenance and hardware or software upgrades.
Customer-Facing IT Services
• Technology-based services.
• IT-enabled business processes.
• Examples such as e-mail, financial systems, and payroll.
Business Processes
• Executed by the business to deliver needed services.
• Examples such as new-hire processes, payroll, manufacturing systems, and sales processes.
Business Services
• Delivered by customers of the business to provide value.
• Examples depend on type of business, such as mortgage services or quality control.

EXHIBIT 12.2 IT Service Catalog Elements

and password, the employee or other authorized stakeholder user would receive this type of a home page. It lists the various systems support and applications areas available. For example, an authorized user might then click on applications monitoring services. These could be special tools to enhance other user-assigned applications, and the (5) notation indicates the number of other related applications available in this category. Although they are not shown here, a click here would retrieve a list of these applications.

A series of further options can also be displayed as part of this service catalog sample page, with links to other pages, including:

- **Service requests.** This would be a catalog listing of the status of user requests to gain access to some new application or other IT service.
- **Problem ticket status.** IT users encountering problems with any type of IT application or service would file some type of a problem ticket document, as discussed as part of ITIL in Chapter 6.
- **Training history.** The home page should report on the status of training programs available to the requesting User ID.
- **IT department contact links.** This would be a general help link.

Because any such service catalog will not cover all user requests, the enterprise should have a ticket process in place where users can both file special requests and verify the status on any filed tickets. In addition, accurate records should be maintained for training activities. It is important to demonstrate that certain employees have received training for key applications and that they have completed the requirements of that training.

A service catalog might also be organized with a series of special panels with links to applications or services available to the employee user. Such a list would be flexible depending upon the users' login rights. A supervisor from field marketing, for example, would only see links to applications that he or she is authorized to access. Other panels would provide the user with help desk contact numbers, important systems news, and virus and security status information. IT security issues are discussed in Chapter 10, and systems should be in place to inform all users of the current status of virus and security issues.

The left-side panel on this sample home page contains a list of services that would be available to the user based on his or her access rights login IDs. These would typically be special-request types of applications that are not part of a user's regular daily activities but may be needed for special requirements.

An IT service catalog can be an important tool to organize and even somewhat control access to IT resources in an enterprise. Senior managers and their IT functions should be encouraged to implement effective service catalogs that will allow all impacted enterprise stakeholders to make effective use of the IT resources within their realms of responsibility.

IT SERVICE CATALOG MANAGEMENT

Perhaps because of the enthusiasm of IT vendors and the IT technical press, IT service catalogs have been "trendy" things to implement for many enterprises over

EXHIBIT 12.3 Global Computer Products Service Catalog Home Page

Global Computer Products

Information Technology Division

IT Service Catalog Home Page

User-ID:	Password:

FIND a Service: _____. A–Z Listing | Recently Added | Print Version

- Application Services (5)
  Application Monitoring Services, Call Center Management (Operator Services), Custom Application Development
- Communication/Collaboration Services (23)
  ActiveSync Wireless Messaging Services (iPhone, Windows Pocket PC, Palm, smartphone), BlackBerry Wireless Messaging
- Connectivity Services (10)
  Paging Network Support, Cable Management—Inter/Intra Building Connectivity, Consolidated Network Monitor
- Enterprise Applications IT Support (3)
  Business Intelligence Services, Enterprise Application Services, Enterprise Directory Services
- Hosting Services (7)
  Co-Location Services, Database Hosting Services, Google Search Engine Service, Mainframe Hosting Services
- Infrastructure Services (13)
  Active Directory Development and Testing Services, Active Directory Management and Operations Services, Desktop
- Professional Services (5)
  Consulting Services, General IT Security Services, IT System Security Assessment and Authorization Relationships
- Support Services (10)
  Deskside Support Services, eDiscovery Services, Media Sanitization Service, Messaging and Infrastructure Support
- Training Services (3)
  Custom IT Training, IT Training Facilitation (Classroom Rental), IT Training

Please contact the Global Computer Products IT Service Desk if you need any additional information about services in this catalog.

recent years. However, spending time and resources on such an application is of little value to an enterprise unless the effort has been effectively planned, implemented, and managed throughout an enterprise. Service catalog management processes provide IT with control over internal initiatives to develop, deliver, and support services while establishing a partnership with its consumers who will receive the agreed services at expected levels and price. The benefits of effective IT service management include:

- Creating a service-driven culture that elevates the perception of the IT organization from just another department to a service provider.
- Providing a source of reliable information to better manage IT investments.
- Increasing customer satisfaction by allowing them to choose correct levels of IT services for their needs.

IT organizations or functions should marshal their resources, with senior management approval, to produce and maintain an IT service catalog containing accurate information on all services and those being prepared to be run operationally.

Such a service catalog development effort should bring significant benefits both internally and externally to IT. Internally, IT organizations should develop and release services according to the requirements derived from enterprise business strategies. Externally, IT consumers can better understand IT direction and request services and service levels that IT is ready to produce.

The steps to establish an effective IT service catalog and to effectively manage these processes include:

- **Document IT's definition of service.** Gaining an agreement and documenting the definition of IT's services is the first and probably the most challenging step here. The question for both IT and user management here is, "What is an IT service?" This question is not easy to answer and an IT organization can potentially spent a lot of time to come up with a clear definition. ITIL, introduced in Chapter 6, provides a good clear definition: "A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks."

  The triggers to effective service catalog management processes are the monitoring and understanding of changes in the business requirements and services. The IT organization should receive business information input from the organization's business to develop IT strategy and financial plans based on current and future requirements from IT's current service portfolio. This will allow the service catalog to accurately describe the services that will need to be published. Information here might include agreed-on details about service levels, time-to-market issues, and changes in basic business processes that rely on the IT services.

  The definition of the services would also include the business units that will be able to request the service and the business owner and service manager who will approve the requests. The documentation should include the details and the status of all operational services and those being transitioned to the production.
- **Build the catalog contents.** Once the service definition and all related information are documented, IT can establish their service catalog content, an activity that includes how to organize the service offerings and how to present all of the agreed details to the consumer.

  This may result in unforeseen difficulties because of the complexity of some service definitions. We should remember that a "service" can include other activities such as IT infrastructure components, including hardware, applications, networks, and data. It can be very helpful to define a hierarchy of services within the service catalog, by qualifying and grouping the types of services recorded, including

business, supporting, infrastructure, network, and application services. Asking customers which IT services they use and how those services support their business processes can be a very good way to facilitate this activity. Developing and completing an IT service catalog definition template, as shown in Exhibit 12.4, can start this process. Completing these predefined service definition templates and distributing them for review and approval among the main stakeholders will facilitate the task.

- **Establish business service views.** As part of developing a catalog of IT services, there is a need to understand the business service views. This includes the details of all the IT services delivered to the customer, with descriptions and details that the customer understands, together with relationships to the business units and the business processes that rely on the IT services. The business service view is the customer view of the IT service catalog and facilitates the development of a much more proactive service level management process.

  Technology solutions can help to generate the business service views, allowing IT to decide which services can be selected, how many times, what are the possible combinations of options that can be associated to a service, and the service levels that can be requested.
- **Establish technical service views.** Because of the structure of IT services, there are many supporting services that are and should remain completely invisible to the IT users or customers, but are essential to the delivery of IT services. A technical service catalog is different from the business view, and it contains details of all the IT services delivered to the customer, together with relationships to the supporting services, components, and configuration items necessary to support the delivery of the service to the business.

  Many enterprises decide to maintain only a business service catalog or just a technical service catalog. However, a preferred situation adopted by more mature

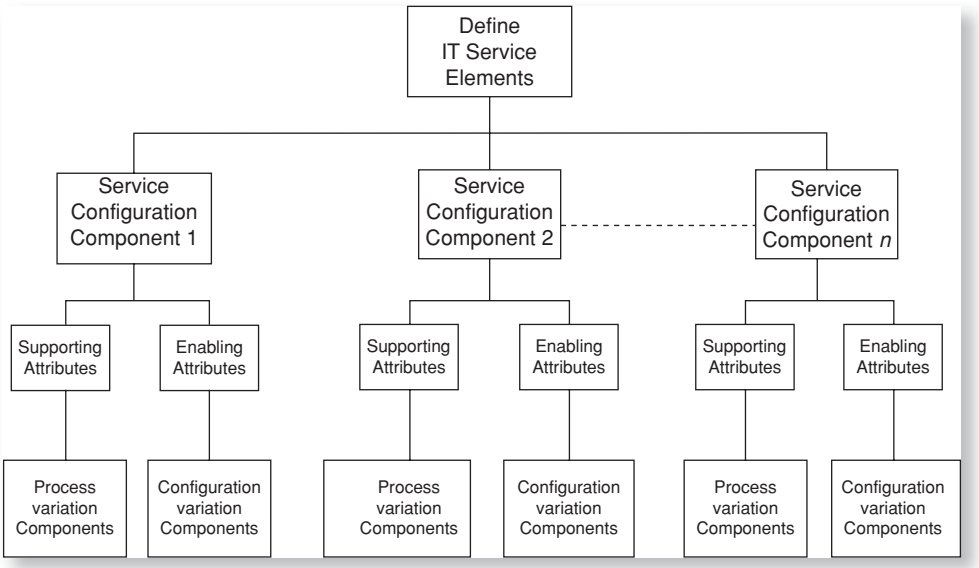

EXHIBIT 12.4 IT Service Catalog Definition Template

enterprises maintains both aspects within a single service catalog that is role-based. It allows different users to access the business and/or the technical views.

- **Publish the service catalog live services.** As a last step and very important management function, an IT organization should publish its service catalog to its customers. The adoption and development of a Web-based interface to allow access to the offered services is the natural solution here. Exhibit 12.3 depicts such a Web service catalog home page.

  It is good practice to perform usability studies and performance tests well in advance, taking into consideration the many types of employees and levels that could exist within the enterprise's structure. It is important to consider the roles that users have in their business units and organization policies. The service catalog should be constructed to easily allow users to create a service request on behalf of themselves and others, and contain facilities to approve service requests. These aspects of a service catalog can make the IT organization's life much easier in facilitating the introduction of a new system.

  Before launching any IT service catalog, both IT and key users should test all aspects of the product, similar to the quality assurance reviews necessary to any new initiative. Testing the service catalog implies testing technical functionality, which is objective in nature, as well as more subjective usability testing. Both are important to the overall success and adoption of any IT service catalog.

  An IT service catalog is an important management process responsible for producing and maintaining a description of all IT services. The information contained in a well-planned and well-organized service catalog should be prepared to be run operationally and ensure that information on agreed IT services is widely available to those who are approved to access these services.

  Technology can play a critical role in optimizing the service catalog management process, by automating the actual process activities themselves and building service offerings through the business unit structure, and by accessing the outputs from other related processes. An effective and well-managed IT business service catalog is an effective element of good IT governance.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

PART FOUR

Building and Monitoring Effective IT Governance Systems

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER THIRTEEN

Importance of IT Service-Oriented Architecture for IT Governance Systems

PROFESSIONALS WHO HAVE BEEN WORKING with IT systems and applications over the years know that IT technologies and techniques are always changing and evolving. What was a hot new concept just a few years ago often soon goes away and is replaced by something else new and completely different. In other cases, concepts that once seemed too advanced or even strange soon evolved into normal accepted practices. Client–server computer system configurations are an example of the latter. They were a new and different concept in perhaps the mid-1990s but are now the standard language of IT. Managing IT applications through service-oriented architectures (SOA) is another relatively new concept that will soon become part of the standard language of IT. We are using the abbreviation SOA although others sometimes use the name software as a service (SaaS) as well. They both mean about the same thing, and we will use SOA throughout these chapters as we explain the concept.

SOA is an IT systems approach where an application's business logic or individual functions are modularized and presented as services for consumer/client applications. A key concept is that the actual IT services provided are loosely coupled and independent of an actual application implementation. As a result, IT developers can build applications by selecting and grouping various IT components to form new applications, analogous to the ways a child takes the various pieces of a LEGO[1] toy set to build a new structure.

This chapter will introduce SOA concepts for IT systems and applications and will discuss internal control and IT governance issues surrounding the development and operations of IT applications using this technology. SOA is a strongly evolving concept for IT applications development and implementations today. When an enterprise's IT function professionals talk about *SOA* and use the term as a new buzzword, business managers should have a general understanding of the concept as well as the internal controls and concepts surrounding SOA implementations.

SOA APPLICATIONS AND SERVICE-DRIVEN IT APPLICATIONS

Hardware and software vendors, as well as high-level software application developers, often use similar but slightly different terms to describe SOA concepts. We may encounter such expressions as service-oriented architectures, service-oriented design, and object-oriented design when hearing about the attributes of some new IT application. These expressions sound alike and generally reflect similar approaches to the manner in which IT applications are built and launched in our Web-oriented world today. In this chapter, we will generally use the expression service-oriented architecture to describe this concept even though computer science purists may differ on some terminology details.

SOA is an IT architectural style whose goal is to achieve loose coupling among interacting software agents. To help with definitions, loose coupling describes how multiple computer systems, even those using incompatible technologies, can be joined together for transactions, regardless of their hardware, software, and other functional components. For example, computers in a network are considered loosely coupled systems since a client machine may request data from a server, even though the two systems also work independently of each other.

SOA allows interoperability between different IT systems and programming languages, providing the basis for integration between applications on different platforms through messages across network communication links. The software is built following both common and industry-specific standards that are granular and modular components. A service is a unit of work done by a service provider to achieve desired end results for a service consumer. Both provider and consumer are roles played by software agents on behalf of their owners.

While this description may be too abstract for some, SOA is really not that difficult of a concept. The music CDs in our homes as well as our CD players model SOA concepts. If you want to play a CD, for instance, you put a selected CD into a CD player and the audio unit plays it for you. The CD player offers a CD music-playing service. When the CD ends, you can replace one music CD for another. You can also play the same music CD on a portable player or on a unit in your automobile. They both offer the same CD playing service, but the quality of service may be different due to differing sound projection systems in each. The results of the CD music-playing service may result in a change of state for the listening consumer, perhaps a mood change from depressed to happy. We are the service client, the CD player is the service provider, and our music library of CDs acts as service broker.

Just as the CD player gives us prerecorded music, the reason that we want someone else to provide services or do the work for us is that they have the available resources and are experts. Consuming a service is usually cheaper and more effective than doing the work ourselves. Most of us realize that we are not smart enough to be experts in everything. The same rule applies to building software systems.

This concept of using the music service of a personal CD player from a library of music CDs leads to SOA concepts. The service is the basic building block of SOA and it is a way of accessing repeatable business capabilities, organized as simple software interfaces available for all providers and consumers. Exhibit 13.1 shows this basic

concept of a SOA configuration, with the service requestor requesting services from a provider or aggregator with a catalog of available service offerings, who will pull the request from any of multiple service providers, who return the service to the requestor and then to the provider. Service catalogs were discussed in Chapter 12, and a basic SOA concept is the taking of an established service catalog and using it to provide requested IT services.

For a service-oriented architecture to be effective, there is a need for all users of IT systems and services to have clear understanding of the term *service*. Sometimes even more importantly, an IT function really needs to understand what it means when it tries to offer IT services rather than the traditional new systems and processes. An IT service is a function that is well-defined, self-contained, and does not depend on the context or state of other services. Services are the building blocks of SOA and can be snapped together to make other services or assembled in sequences to make processes.

In SOA, services are organized in what is called a registry, where separate services can be snapped together to create composite applications and then fitted together into what is called an SOA blueprint. IT management generally encounters SOA efforts when assessing its overall enterprise general controls reviewing specific application controls. While our objective is not to make the reader into a computer scientist or software developer, several important SOA concepts that IT professionals and interested management may encounter when discussing SOA processes are:

- **SOA component granularity.** Describes the size of the components that make up a system. An SOA implementation would try to achieve larger or coarsely grained components known as business services. These would usually be built out of smaller or fine-grained components as well as preexisting technical services. This concept matters because larger-granularity chunks make SOA services easier for an enterprise to understand, reuse, and manage.

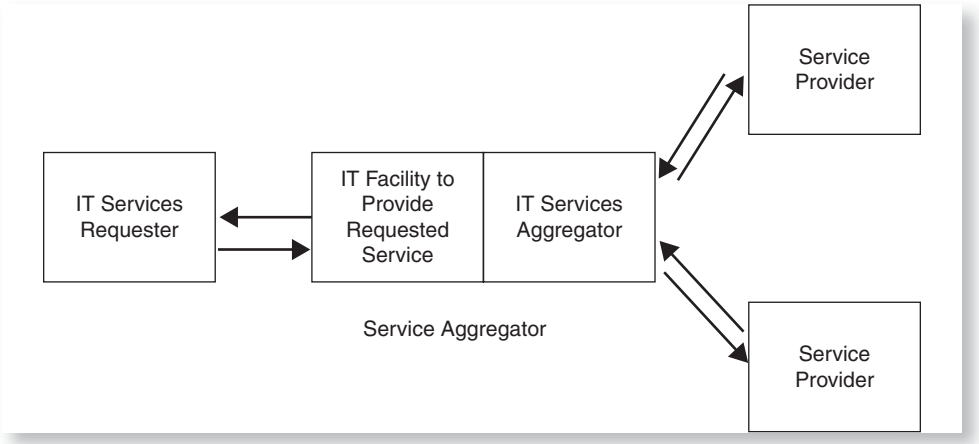

EXHIBIT 13.1 Role of the SOA Service Aggregator

- **Service interface versus implementation concepts.** Separates *what* a service does from *how* it does it. This matters because it simplifies the concept that the business user's view of SOA should focus on what the service will do rather than the details of how the technology works under the hood, using an automobile analogy.
- **SOA contracts.** Define the obligations between the *service provider* and *service consumer* or *requestor.* This can include service expectations like availability, reliability, key performance indicators, cost, and support. This matters because it helps business users make rational business decisions about which services they can rely on. These concepts are similar to the service level agreements discussed in Chapter 17.
- **SOA loose coupling concepts.** These are a way of designing services that are more flexible and less dependent on each other. This helps services to snap together or couple and recombine. An SOA environment with loose coupling matters because it is faster to assemble business solutions out of premade blocks than it is to write every new business function from scratch.

Adopting SOA in an enterprise is not a one-application-at-a-time process but an overall architecture where all IT processes are organized together and connected. Services provided with Web applications where a user just double-clicks to pull up an HTML reference are an example of an SOA concept. Exhibit 13.2 illustrates a hypothetical enterprise-wide SOA configuration.

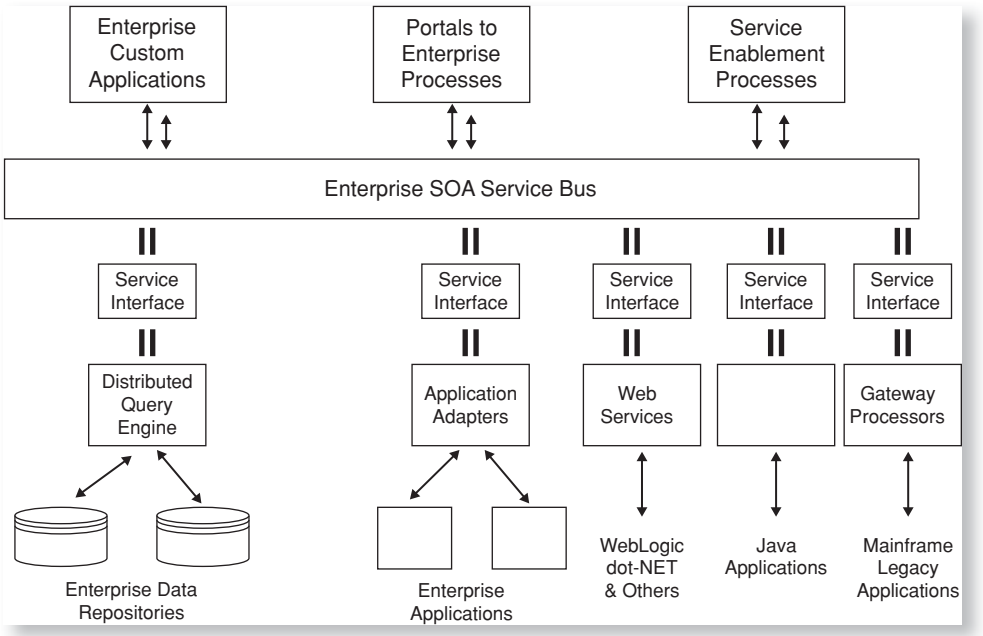

EXHIBIT 13.2 Enterprise-Wide SOA Configuration

At the lower level of the exhibit are enterprise data sources and other multiplatform systems. All elements would be defined as services such that a custom application, for example, might be built of a combination of server, mainframe/legacy, or Web application components and assembled with the requested components through a service bus to the proper adaptor and application. When any of those application services needed an element of data—another service—a request would go up to the communication bus and back to the appropriate data source. Such an overall application would be built using vendor-supplied application software development tools such as Microsoft's dot-Net[2] or Oracle's BEA WebLogic[3] and would be configured and orchestrated in clearly specified processes.

An interested enterprise executive will often not find such a full SOA environment in the typical enterprise. Rather, an enterprise IT function with the support of its management will typically implement an SOA environment on a step-by-step basis following an overall blueprint to build that model. With the growing use of Web services surrounding most IT environments and software sold and delivered as individual program components rather than full applications, senior business managers can expect to see many partial and even full SOA implementations going forward.

SOA GOVERNANCE, INTERNAL CONTROL ISSUES, AND RISKS

An enterprise does not move to an SOA IT environment just by purchasing a software package, training the IT staff on its use, and then assuming they are off and running. SOA is more than just a new way of organizing existing IT systems, and it requires detailed planning to move to that new environment as well as new IT policies and procedures. Even more important, it requires a gradual and very structured implementation where IT processes are brought into an SOA environment in a controlled manner. In some cases, the advantages of SOA operations will be obvious to senior managers and others. For example, an enterprise that has moved a large segment of its applications to a Java or dot-Net Web-based environment can often easily justify the advantages of moving its legacy applications and other processes to an SOA environment.

Involved senior managers should develop a good but general understanding of SOA processes as well as some of the steps necessary for enterprise management and their IT functions to transition to SOA processes. Part of this requires an understanding of IT governance internal controls, as discussed in Chapter 4. Senior managers should also be comfortable with IT infrastructure controls in an SOA environment as well as understand good project management controls, as discussed in Chapter 16. The interested senior manager needs to understand the somewhat unique characteristics of SOA and its governance, internal control issues, and risks. This chapter will briefly discuss implementing effective SOA processes, from an IT governance perspective. The following sections will discuss the importance of building a planning blueprint for an SOA implementation, cleaning up existing applications and processes in advance, establishing appropriate SOA policies and procedures, and testing and implementing SOA in an effective manner.

PLANNING AND BUILDING AN SOA IMPLEMENTATION BLUEPRINT

The third letter of the acronym SOA stands for *architecture*, and the building of an effective architecture is an essential early step to launch SOA in an enterprise. An enterprise chief information officer (CIO) may have been exposed to its concepts, or the enterprise may have implemented an SOA-like single application that gained lots of enthusiastic comments and praise, but an enterprise needs to build an overall plan or framework to launch any SOA process implementation.

The key to an effective SOA is to identify an existing plan or build the service using building blocks that will define the SOA. As discussed previously, SOA services should be viewed similar to a series of LEGO building blocks, the popular children's toy where the blocks can be interconnected in a variety of elaborate structures and then disassembled to build a different structure. However, SOA services are more than LEGO blocks that may only be in cubical and triangular shapes; SOA services are much broader and generally may have many different dimensions. An enterprise SOA should to define its various service elements and the service stakeholders, including the flow of activities and decision points between the stakeholders involved in the process, as follows:

- **Business owners.** The owner or systems user provides the application requirements for a new business capability, solution, or process to be implemented. A business owner or supporting IT staff members should develop process models to make any understanding of IT implementation service requirements easier. The business owner also needs to define nonfunctional requirements, such as expected quality of service, for the capability, solution, or process.
- **SOA architects.** In order to launch an SOA initiative, an enterprise needs to designate a skilled SOA architect to analyze the business requirements and break them into service and process designs. The SOA architect may decide, for example, to reuse existing components rather than create new ones. When the architect proposes a new or changed service or process implementation, the SOA architect should deliver design specifications in terms of state diagrams, process models, and interface designs. The SOA architect formalizes the nonfunctional requirements of the component to be implemented, including its availability, security, and performance requirements.
- **Application developers.** An application developer implements components based on the design specifications delivered by the SOA architect, establishes internal controls, and creates test plans based on these specifications. To aid in the convergence of technology and methodology, an application developer should use parts generated by the SOA architect for implementation, including code generation or model refinements.
- **Quality manager.** An enterprise quality manager should use the inputs provided by the business owner, architect, and developer to review the correctness of the service or process that was implemented. A quality manger then uses the test plans provided by the developer to execute a solution test in a staging environment and validates quality metrics, side effects, and nonfunctional characteristics.

Once a key team has been identified, the enterprise should develop an SOA blueprint that indicates a target state or a complete picture of what the SOA implementation should look like when it is completed. The SOA blueprint should primarily outline each of the business services to be performed, the related service description requirements and performance metrics, and interoperability standards.

Such a blueprint provides an overall outline and even "marching orders" of where enterprise and IT management want to go with SOA. Of course, an enterprise should not begin to implement or even approve an SOA strategy unless there is a good understanding of the benefits to be achieved from the approach. Exhibit 13.3 describes some of the key benefits that an enterprise should realize from moving to an SOA environment.

Transitioning Current Applications and Processes to SOA

The transition of existing processes or applications, whether they are older legacy systems, server-based applications, or more recent Web-based mobile applications, has some of the same challenges that some older professionals may recall during the late 1990s from the Y2K scare. Although most professionals have now forgotten, many COBOL language–based programs developed in the 1990s, 1980s, or earlier had system calendar date fields in a *yymmdd* format, and many date-difference program code decisions were based on taking system actions by sorting on those dates. The year 2000 caused those date-based program decisions to be recorded as 0000. The concern was that many systems would fail because of bad, out-of-sequence program dates, and many

EXHIBIT 13.3 Key Benefits from Using SOA

The following are points that IT and general management should consider in moving their IT systems and services to a service-oriented architecture (SOA)

Improve Business Visibility. SOA generally integrates existing systems and aggregates data for more consistent, accurate views of customer data, including:

- Up-to-the-minute information for improved customer service.
- Cross-enterprise information for targeted 1:1 activities.
- Consistent, accurate, and more comprehensive information for better decision making.

Achieve Business Flexibility. Fully implemented, SOA can create an integrated, agile software infrastructure for quickly responding to business needs:

- Rapid delivery of new business capabilities.
- Reduce impact of business and technology changes.
- Protect investments while creating new functionality.

Gain Business Efficiency. Streamline, automate, and enable the better tracking and visibility of enterprise business processes:

- Securely share business processes inside and outside the IT systems firewall.
- Bridge silos of data to better ensure data integrity.
- Proactively manage business decisions with key performance indicators from other sources.

Improve IT Governance Processes. Because SOA better classifies and organizes all IT processes for an enterprise, the overall governance and control of these processes is better managed and controlled.

older applications at the time were poorly documented. IT functions and IT auditors went through major efforts to get ready for Y2K.

IT functions face some similar issues when planning an SOA conversion. While the concern today is not on undocumented *yymmdd* format COBOL dates, the typical IT function has layers of IT applications and programs, redundant and often mutually inaccessible systems, and many jumbled point-to-point integrations for its applications. These problems represent perhaps the biggest challenges to implementing effective SOA processes. If any team implementing enterprise-wide SOA does not understand the existing IT systems, processes, and organization structures, there is a strong possibility that the SOA implementation will fail.

SOA Policies and Procedures

The overall concept and beauty of SOA is its use of service units that can be assembled and reassembled following the previously referenced example of the LEGO blocks. However, SOA will not work very well for an enterprise if one or another business unit decides it wants to be a bit different and that its service units do not really fit with others. Using our LEGO block example, some unit might want its blocks to be of a different size such that they do not fit with any others.

While there are always reasons that one or another unit needs to be different (e.g., high security issues), an enterprise normally needs some type of standards-setting authority to establish policies and set the rules for its SOA services. For many enterprises, governing bodies that create and enforce SOA policies and enterprise standards are typically called the *SOA centers of excellence* or *SOA competency centers.* These competency centers often consist of representatives from each of the business units that are affected by the enterprise's SOA blueprint and plans. Almost every part of an enterprise SOA blueprint—including which services will be built, how they will be defined, and how they will interoperate—implicitly defines the SOA policies for an enterprise. Because the SOA blueprint typically contains many implicit policies, it is important that the first act of a newly constituted SOA competency center be to ratify this blueprint as a shared goal.

Of course, it is important for each affected enterprise group to understand and agree to the implications of the SOA blueprint as it impacts their daily work activities. For that reason, ratifying an SOA blueprint should not be a rubber-stamp activity. Everyone involved should think through how this SOA vision will affect them, including overall IT governance implications.

An enterprise should develop compliance procedures to monitor and assess the enforcement of its SOA policies and processes. This establishes "rules of the road" and provides governance for SOA activities, based on the approved blueprint. Automated enforcement processes are preferable to manual enforcement, where it can be established. However, not all policies can be automated, and some steps may require human judgment and intervention.

Proper SOA governance covers multiple enforcement points across the entire service life cycle. Exhibit 13.4 describes the roles and responsibilities of key persons involved in implementing SOA and being part of its particular systems development life cycle. Systems development life cycle (SDLC) concepts and their importance in IT governance

are discussed in Chapter 15 on implementing integrated IT systems. SOA policies and processes are usually divided into two categories: (1) design time governance policies to ensure that SOA artifacts meet the design requirements set forth in the SOA blueprint, and (2) runtime governance policies to ensure that SOA services meet the runtime requirements negotiated between service provider and consumer. These SOA governance processes are somewhat like the service level agreements (SLAs) discussed in Chapter 17 where IT operations will formally agree to provide user group input transactions according to a pre-agreed schedule and IT will deliver file updates and completed processes according to the same type of contracted schedule. With SOA, we are making a series of small agreements between service providers and consumers.

EXHIBIT 13.4 Stakeholder SOA Life Cycle Roles and Responsibilities

An SOA life cycle describes and implements a flow of activities and decision points between the stakeholders—users and IT—involved in this process. The SOA development life cycle should recognize the following key participants:

- **Business owners**. The SOA business owner provides the requirements for a new business capability, solution, or process to be implemented. The best way to express these requirements is in the supporting process model covering the service activity. Using process models provides an environment that makes understanding IT implementation requirements easier. The business owner also needs to define nonfunctional requirements (such as quality of service) for the capability, solution, or process.
- **SOA architect**. The SOA architect, usually as key member of the IT team, analyzes the business requirements and breaks them into service process design elements. The architect may decide to reuse an existing component rather than create a new one, in which case the SOA architect will decide to turn the requirement into an element in the SOA life cycle in order to reuse the existing component. When a new or changed service or process implementation is identified, the SOA architect delivers design specifications in terms of state diagrams, process models, and interface designs. The SOA architect formalizes the nonfunctional requirements of the component to be implemented, including the availability, security, and performance.
- **SOA developer.** The developer implements components based on the design specifications delivered by the SOA architect and also creates test plans based on the specifications. To aid the convergence of technology and methodology, the developer uses the parts generated by the SOA architect for implementation, including code generation and model refinement tools.
- **SOA quality manager**. The quality manager uses the inputs provided by the business owner, architect, and developer to review the correctness of the service or process that was implemented. The quality manager then uses the test plans provided by the developer to execute a solution test in a staging environment and validates quality metrics, side effects, and nonfunctional characteristics.
- **SOA operator**. An SOA operator receives the tested and validated solutions and implements them within the standard IT processes in order for the solution to be made available to the users and consumers of the solution. He or she uses the formalized nonfunctional requirements specification in order to operate a virtualized solution that complies with the service level agreements (SLAs) required by the application consumers. SOA runtime governance solutions provide these kinds of capabilities by enforcing nonfunctional requirements and SLAs.

SOA Design-Time Policies

A key component of SOA policies and processes, design-time policies, ensure that services are built to meet the specifications outlined in the SOA blueprint's plan. In particular, policies should be tailored to constrain the behavior of service designers and developers on behalf of the whole SOA effort in the following broad areas:

- **Interoperability.** An SOA blueprint should declare a uniform means to provide interoperability among the IT services, typically by ratifying a set of standards.
- **Discoverability.** Services may require specific attributes such as a business friendly description and information regarding the location of the service within an established classification or registry catalog. These elements make it possible to discover services that can be further defined through policy.
- **Security.** The SOA blueprint should declare a uniform means to provide security across all SOA services. The style and parameters of this security should be consistent with overall enterprise IT security governance practices, as discussed in Chapter 10.
- **Uniqueness.** Services should not have the same name as other preexisting services. Policies can help ensure that groups do not run into this problem.
- **Interface compliance.** All SOA services should require a uniform way to use or initiate them. Although SOA services are more than just IT program elements, this process is similar to a Microsoft Windows Run command. This standard form of interface should be mandated by policy.
- **Data format compliance.** As discussed, a major objective of SOA services should be the reusability of service elements, and a common way to endure their reusability is to establish common data formats known as schemas. Doing so ensures that an address field in one service can be properly used by another service, even if differences exist in how the services store the data. Common schemas should be mandated by policy.
- **Metrics.** Statistical information and reporting of service design issues should also be set by policy. An enterprise, and certainly IT audit, cannot measure the effectiveness of SOA operations unless some metrics have been established as both goals and operating minimum performance standards.

Design-time SOA processes should typically connect with the enterprise's system development life cycle (SDLC). The SDLC process and its importance for IT governance will be discussed in Chapter 15 and a similar service development life cycle can be developed here. SOA adoption presents challenges to enterprises that are accustomed to using IT implementations as a way to address application requirements. New structures and processes, typically referred to as the SOA life cycle, are required that provide the basis for organizational agility and promote successful SOA adoption. SOA life cycle processes, combined with effective organizational structures, become key elements in launching effective SOA processes.

Most enterprise IT departments are under high pressure to deliver cost-effective and timely solutions to their business operations. To achieve these solutions goals, they use shared technical and organizational components and functions, as well as cross-project

initiatives to strengthen synergies across the IT department. When these solutions are combined with a mind-set to deliver services (as in a valuable service and not as in technology), an IT function can find itself moving onto a path to SOA.

As part of this path to SOA, all parties—IT and management—should have a mind-set that thinks in terms of value chains and understands that service is something that exists to deliver consumer satisfaction. Although it is admittedly easier said than effectively implemented, an enterprise needs to break up what is traditional application-centric thinking by implementing structured processes that cross project boundaries and their life cycles. When mind-set, methodology, people and organization, and technology are successfully combined, SOA adoption can lead to great benefits for an enterprise in terms of scale, efficiency, and especially agility.

SOA Runtime Policies and Processes

Runtime includes the overall process of the development, staging, and production of SOA systems. Runtime governance policies will produce a reduced level of political friction in an enterprise because they mostly constrain IT systems on behalf of SOA service consumers. For the most part, runtime policies exist to ensure that services behave how they are "supposed to" following the expectations of the service consumer. These include:

- **Service level agreements.** SLAs are discussed in Chapter 17. SOA providers and consumers should agree on SLA performance expectations as well as measurements that confirm that services are performing as expected.
- **Authentication.** Providers and consumers should also agree on how service consumers should identify themselves. Based on runtime governance standards, authentication should include such issues as the identity systems and security tokens used.
- **Authorization.** Security processes should be in place to determine if a provider is allowed to invoke a service.
- **Encryption.** As part of strong security processes, there should be encryption standards to keep messages coded or scrambled so they cannot be easily read by the wrong people.
- **Alerts and notifications.** Conditions should be established to trigger alerts with procedures to send them to proper authorities. Alerts can signify both business and technical conditions.
- **Metrics.** Runtime key performance indicators and measurements should be established to provide indicators that can later be used to assess performance.

Runtime policies typically constrain the IT operations team and IT systems on behalf of the service consumer. These processes can include support requests and responses to real-time alerts and notifications. Enabling a more responsive request for changing runtime conditions is an important value in SOA.

Like the customs checkpoint at a country's border that inspects both passports and luggage, an effective SOA governance process sets up checkpoints to ensure that agreements between organizations are being enforced, including an SOA registry

repository to serve as the enforcement point for SOA design-time policies and processes. The controlling software system should have facilities to serve as the enforcement point for SOA runtime policies and processes, including message validation processes to ensure that they are authorized to invoke a service, an important operational requirement.

We have emphasized the importance of SLAs in several places in our discussion of SOA processes. Well-defined and well-monitored SLAs keep an eye on service health and performance and ensure that services are delivered as promised to consumers.

The SOA requirements or attributes mentioned in the preceding paragraphs change far more frequently than the functional logic of a service. Senior managers should realize that a core mission of SOA governance is to promote and ensure desirable behavior among its participant people and systems. IT management must clearly communicate its SOA policies and then must enforce these policies consistently throughout the SOA life cycle.

In the early days of SOA, its architects would spend weeks or even months painstakingly documenting policies in fat books that no one cared to read. This is similar to the early IT disaster recovery plans, now called IT continuity plans, discussed in Chapter 10. If getting participants to be aware of these policies was not hard enough, communicating changes to policies was even harder. Those older manual review and approval processes had to be put into place to force everyone to read and comply with the latest rules. Such reviews quickly became bottlenecks and encouraged people to go around policies, defeating the core mission of SOA governance.

While true for all IT policies, strong and effective SOA policy management practices are particularly important here. While really IT management's responsibility, enterprise SOA policies should be expressed in declarative formats that can be easily defined, changed, and removed as needed. In addition, processes should be in place to actively enforce those SOA policies, as applied throughout the SOA life cycle. Participants receive immediate feedback with policy management, a critical component of SOA governance processes.

Effective SOA policy management removes hurdles and objections to SOA governance by providing clear guidance regarding what is expected to be compliant with the established and approved SOA blueprint. Policy management solutions improve accountability and ensure consistent outcomes.

SOA AND IT GOVERNANCE

We have discussed many IT governance aspects of SOA, but unfortunately have only discussed a few of SOA's many attributes and features. With its concept of breaking down software elements and functions into independent and interchangeable components that can be easily connected or redefined, we will see more and more SOA-related functions in our Web-centric world going forward. For example, major database software vendors today, such as Oracle, have implemented SOA principles in their enterprise resource planning database structures, and we should see a greater SOA emphasis on their products over the years.

The typical enterprise using a full spectrum of SOA tools today will almost certainly not initially begin operating following the full SOA implementation model. Rather, many

enterprises even today have converted one or another key application to a Web services model, an SOA-like approach. That Web services application process of converting an existing application into a Web-based and Web-dependent environment is shown in Exhibit 13.5. An example of this type of applications can be found in one of the customer relationship management software solutions offered by SalesForce.com (www.salesforce.com/company), a very successful software provider that does not sell its software products through a CD containing the software and a three-ring binder with the documentation. Rather, everything that SalesForce.com offers is in a Web format.

Rather than individual, separate applications, Web services applications are different. Application components communicate with one another over the Web and on other applications using open communications protocols. They are self-contained and self-describing and can be used by other applications. Managers will almost certainly encounter increasing numbers of Web service applications in the future. Various resources will be located in what we call an IT "cloud," storage connections to multiple files, data sources, and other materials. One can think of Google when we consider this cloud concept, where a user can get some form of multiple search results no matter the topic area requested. Web service applications may be linked to this Internet cloud

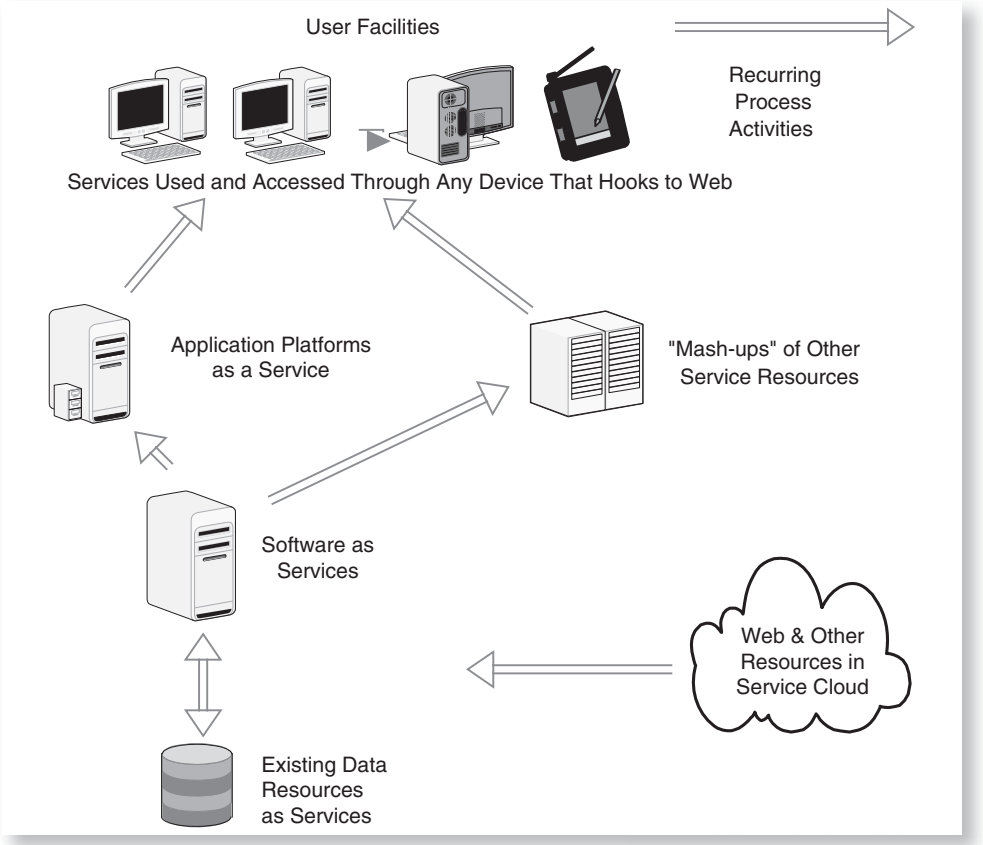

EXHIBIT 13.5 Web Services Application Model

as well as to their own storage resources with ongoing connections to local systems, whether local networks or wireless. The overall concept of cloud computing, as it applies to IT governance, is discussed in Chapter 9.

An enterprise SOA environment today may consist of either a largely implemented total system environment or a project in development that is converting some existing or new applications to SOA. Both face some major governance controls concerns, and senior managers who understand IT general controls following a more traditional IT systems approach will need to rethink these review approaches. Following our earlier LEGO blocks example, we will need to review the controls and governance procedures following these many separate components, including the controls and permissions surrounding each individual component and their interconnections.

Perhaps the major IT governance issue in this SOA environment is the need for a comprehensive SOA blueprint covering all service elements agreed to and approved by all participating parties. These service unit considerations often go beyond just one operating division, beyond the overall enterprise, and may branch to other service providers or suppliers. A strong system of permissions as well as controls within each service element is needed. Again going back to our LEGO blocks example, each service unit should be considered as one of those blocks, perhaps a combination of program elements or data resources. A business unit should make the nonproprietary elements of each of those blocks available to others through clear disclosures and permissions. There should be some level of SOA architect function in place to review these service elements and establish supporting rules and procedures.

Strong infrastructure best practice procedures, as discussed in Chapter 7 as part of ISO standards, are essential in an SOA environment. SOA platforms are not just launched by implementing everything in an all-at-once mode. Rather, service and processes will typically be added, modified, or deleted on an ongoing basis. The challenge is far more complex than individual program library controls, however, where the concerns will be regarding one program element in an application. Under SOA, these changes are to a service unit that can be part of numerous other processes where the owner of a given service may not fully understand who else is using that service element. A control problem in one service may have an impact on many others. There is a need for strong testing and quality controls.

Many of the general IT governance procedures discussed in other chapters are also applicable in a SOA environment. For example, the COSO internal controls framework discussed in Chapter 4 and the security management IT governance controls discussed in Chapter 10 are equally appropriate in an SOA environment. While these other controls are appropriate in a variety of environments, Exhibit 13.6 outlines IT governance controls in an SOA environment. These procedure steps outline an environment where the enterprise is not 100 percent SOA consistent but is moving to that environment through an ongoing implementation project that follows an approved blueprint.

This chapter has discussed SOA as a special set of IT governance processes. However, as we move IT systems and processes more and more to a Web services environment, SOA processes will become the standard and not the exception. Managers need to think of their systems and IT processes following the SOA model.

EXHIBIT 13.6 IT Governance Controls in an SOA Environment

1. Has the enterprise developed and approved a comprehensive SOA strategy for IT and its business operations?
   a. If there is an approved strategy, has it been fully implemented or what is its completion status at present?
   b. If there is no formal SOA strategy, what are future plans for any SOA implementations?
   c. Have there been education programs delivered to introduce the advantage of SOA to both business and IT users?
2. Has a responsible manager been appointed to lead and coordinate enterprise SOA efforts?
3. Has the enterprise obtained or is it evaluating any SOA software?
   a. Have formal evaluation criteria been established to select any software?
   b. For any software in place, has there been a formal testing and evaluation program to analyze the software product for full implementation?
4. Have "mission critical" business applications been identified as part of the SOA strategy?
   a. For any critical applications that are not Web services–based, are there plans in place to convert them to an SOA environment?
   b. Has a formal, mission-critical business process layer been defined and documented for SOA applications?
   c. Is there evidence that the application services layer focuses on integration interoperability, based on database, component, and infrastructure services?
5. Has a formal SOA service director or management team been established?
   a. Have the objectives and risks of this service director been reviewed with management?
   b. Have enterprise SOA plans been explained and discussed with key members of the management team?
6. Is there evidence that SOA plans have been fully integrated with enterprise continuity plans?
7. As the enterprise moves to an SOA environment, are applications initially converted from their regular status to SOA on a test basis?
   a. As part of any test conversion to SOA, are existing application controls reviewed and assessed?
   b. Does any part of an application SOA conversion include testing the component's "plug-and-play" features that are the purported benefits of SOA operations?
   c. Is there evidence that the costs and benefits of any SOA conversion are formally evaluated?
8. Based on testing and evaluations, are all applications converted to SOA consistent with enterprise IT application and system security requirements?
9. On a test basis, have procedures been established and understood by both IT and responsible managers for SOA converted applications?
10. Have the costs and benefits of any SOA conversion been developed and evaluated prior to any full-scale planned conversions?

NOTES

1. LEGO is the brand name for a large number of building blocks and toy figures in different shapes and colors that can be plugged together to create various toys structures and then easily disassembled to create something else. This children's toy product is available worldwide and is a good model of building with component architectures. More information can be found at www.LEGO.com.
2. The .NET or dot-NET framework is Microsoft's comprehensive and consistent programming model for building applications. www.microsoft.com/net.
3. BEA is a unit of Oracle Corporation. Information on its WebLogic application can be found at www.oracle.com/bea/index.html.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER FOURTEEN

IT Configuration and IT Portfolio Management

WHETHER A MANAGER'S IPAD OR LAPTOP, a server system supporting a branch sales office, or the corporate primary data center, any installed IT system will have numerous components, including portfolios of application software, files and databases, operating systems, telecommunications gear, and supporting documentation for these procedures. These IT components should all be connected system by system and across the overall enterprise in order to be able to communicate and work with one another. This whole assembly of IT components is known as an enterprise's IT configuration. As an important element of IT governance, processes should be in place to manage the compatibility and status of these IT configuration components such that they can talk and communicate with one another. An enterprise should have an effective IT configuration management system supporting its IT key processes.

Business managers often encounter IT configuration issues when they receive a report or an error message from some unit of their overall enterprise and find they cannot open or read a transmitted file. The manager's first response often is to call his or her IT function's help desk, but the problem is often traced back to find that the unit sending the unreadable data was using the wrong version of the software or even totally incorrect software. That incorrect and unreadable software problem is often caused by the failure to update a software element somewhere in the corporate IT network. The report or process may work fine at the location where it is currently running but is not compatible with other systems or facilities. This is an example of an IT configuration problem!

Whether it be the data files and programs loaded on an individual's laptop computer or resources somewhere in the corporate IT network, there is a need to maintain consistent and compatible configurations across these IT resources. A change or element revision to one component often needs to be reflected in all other interconnected components. The management of the revisions and versions of these many IT elements

is known as IT configuration management. This area is too often viewed as just an IT technical control, but effective IT configuration management should be seen as an important and necessary IT governance component.

This chapter discusses the importance of IT configuration management processes in all enterprises and outlines key IT governance tools to establish an effective enterprise configuration management system (CMS), with an emphasis on establishing what is called a configuration management database (CMDB). Some elements of IT configuration management processes were highlighted in Chapter 6 on ITIL best practices and IT service management, but this chapter reemphasizes the importance of IT configuration management as an important IT governance control.

This chapter will also introduce and discuss IT portfolio management as an important IT governance concept. Just as many individuals invest in a mutual fund or an exchange-traded fund that contains a portfolio of related securities, there are strong IT governance advantages to managing IT resources on the basis of groups or portfolios of application, infrastructure, project, and related IT resources. We will describe how an IT portfolio management approach for IT investments can yield multiple benefits to an IT organization and the overall enterprise. IT portfolio management is an effective IT investment management approach that can provide a central oversight of IT budgets, IT risk management issues, and the strategic alignment of IT investments. It supports improved IT governance practices.

IT CONFIGURATION MANAGEMENT CONCEPTS

There are multiple hardware, software, and IT infrastructure components in any enterprise IT system, ranging from a database server with attached terminals serving a small business unit to a large, corporate-wide set of IT operations serving worldwide facilities. Some of these are interconnected, while others are freestanding but separate from the others. An enterprise's IT configuration is much more than just a list of installed software components and hardware devices. Configuration records must keep track of such matters as interface connections, component version identifications, installed features, and all other matters that describe these IT configuration elements or items in their installed states.

We first encountered IT configuration management concepts in Chapter 6 on ITIL and IT Service Management Forum concepts. There, IT configuration management was only one element of a series of ITIL's best practices. This chapter looks a bit deeper into IT configuration management tools and processes and will emphasize why IT configuration management is an important component of good IT governance processes.

While there is no one standard definition of an IT configuration management system and a Web search will provide multiple variations as well, the U.S.-based standards-setting technical organization, the IEEE, is a good source for such a definition. Once known as the Institute for Electrical and Electronic Engineering, it is currently referenced by just its initials and is popularly called the "I-Triple-E." Not even its Web site, at www.ieee.org, mentions the organization's original full name. The IEEE defines IT configuration management as an enterprise or IT organization process containing the following elements:

- **Identification.** An IT configuration management process includes a strong identification scheme; reflects the structure of all IT resources; and identifies their components, revision history, and their type, making them unique and accessible in some form.
- **Control.** The IT configuration management system should control the release of all products and changes to the configuration resources throughout their life cycle by having controls in place that ensure consistent IT component resources via the creation of baseline products.
- **Status accounting.** An IT configuration management system should record and report on the status of all configuration components and change requests, while gathering vital statistics about these components in configuration products.
- **Audit and review.** An IT configuration management review process should be in place to validate the completeness of all configuration items and to maintain their consistency among the related configuration components by ensuring that these products are a well-defined collection of components.

The paragraphs following will discuss these elements of IT configuration management and a CMS in greater detail. In order to achieve effective IT configuration management, an enterprise and its IT function should (1) have processes in place to uniquely identify all of the hardware, software, and infrastructure components that are part of their IT resources; (2) have controls in place to keep track of all changes or revisions to these configuration components; (3) maintain a configuration management reporting system such that the IT function, general management, and financial resources understand the present status of an enterprise's IT resources; and (4) monitor and manage the status of these IT resources to determine that they are current and cost-effective.

Effective IT configuration management is much more than just controlling IT program versions through a single, all-inclusive CMDB, and may even include other related resources at one facility, such as the headquarters IT function. IT configuration management processes should encompass the total enterprise, including any facility where there will be a need to communicate or share data and information.

We introduced IT configuration management practices that are part of ITIL in Chapter 6. ITIL best practices cover a wide set of areas, and expanded attention should be given to their guidance for IT configuration management. The sections following in this chapter provide further guidance on establishing IT configuration processes. Exhibit 14.1 describes this CMS concept and the need for IT configuration controls. The chart shows enterprise business systems users in its outer ring, where all need to develop relationships and connections with each other and through their systems resources. These systems users are concerned with the following IT configuration issues:

- **IT asset controls.** Differing user groups and IT functions may purchase and install slightly different versions of software and other tools. Sometimes the differences are generally minor such that an overseas unit will have a slightly different version because of language differences. However, the way the software interprets commands and interacts with other-language versions may differ. How an enterprise

and its operating units purchase and install software and other IT assets may raise configuration issues.

- **Incident management.** The first goal of the incident management process is to restore normal service operation as quickly as possible and to minimize the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. However, "emergency" incident correction activities may miss configuration connections with other units, causing overall longer-run problems.
- **IT problem management.** ITIL defines a *problem* as a condition often identified as a result of multiple incidents that exhibit common symptoms. When multiple systems or user groups encounter the same IT problem, there is a need to get to the root causes of the problem and identify a solution. In a large, complex IT environment, this can become a major configuration problem.
- **Overall IT governance issues.** Chapters in this book have covered a wide range of governance issues, including IT security policies, project management issues, benchmarking metrics, and others. These all should be implemented and managed consistently across an enterprise to ensure consistent and effective configuration management.
- **IT capacity management.** An enterprise needs to install and implement the right levels and loads of IT resources. Processing service needs and volumes need to be monitored and adjusted across all enterprise IT resources.
- **Service level agreements (SLAs).** Introduced with IT governance issues discussed in Chapter 17, SLAs are informal agreements that an IT function makes both with its user communities as well as with outside vendors. In its simplest fashion, an IT function will develop an SLA with the controller's department, where the accounting users promise to deliver all month-end close general ledger system transactions according to an agreed schedule and IT promises to complete and deliver the monthly close reports by a certain date. However, when various user departments and IT facilities all have a need for their own SLAs, there can be CMS problems.

The concept here is that we must think of IT configuration management as a series of often separate but interrelated concepts (see Exhibit 14.1). This is particularly important today where we have moved away from the centralized mainframe of past years and have installed many formats and types of IT resources in the typical multi-unit, multilocation enterprise. While a classic IT function should establish standards over its own as well as headquarters' IT systems and processes, configuration controls can become lost in our world of wireless systems connected to a cloud system.

ITIL BEST PRACTICES FOR IT CONFIGURATION MANAGEMENT

Chapter 6 introduced the Information Technology Infrastructure Library (ITIL) governance materials, and best practices there were illustrated in Exhibit 6.2, showing the importance of configuration management as an IT governance tool. The idea is that

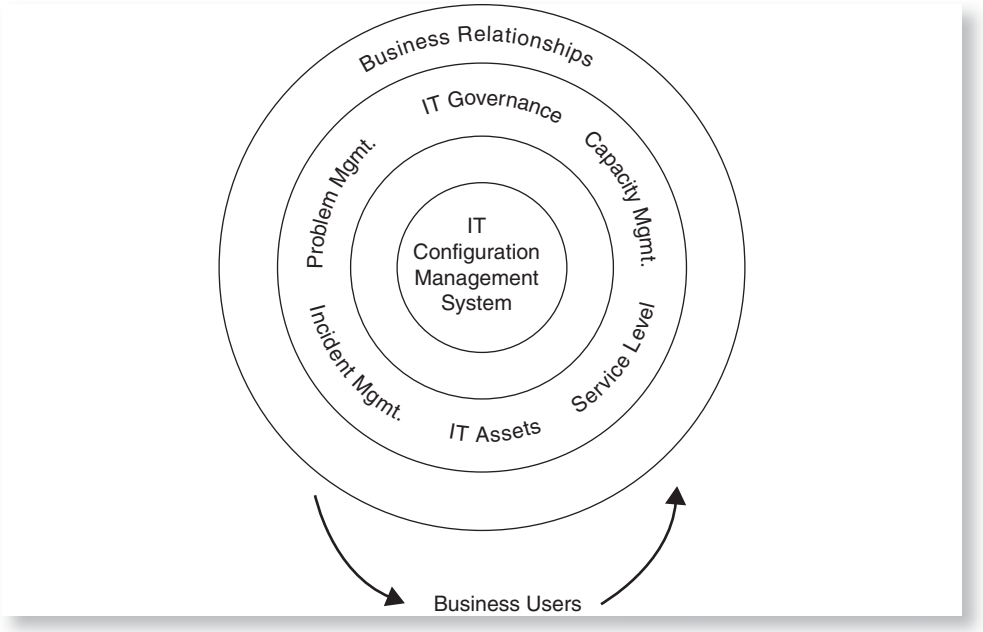

EXHIBIT 14.1 IT Configuration Management System Concepts

every enterprise has or maintains a variety of information elements about its IT infrastructure. However, an enterprise faces a challenge in keeping all of that information up to date. ITIL configuration management defines best practices for keeping reliable and current information details about the IT infrastructure.

Although the term is not a common one to IT operations today, *ITIL* calls for an enterprise and its IT operations to define its configuration structure into what ITIL calls configuration items (CIs) and to understand how these CIs relate to one another. An effective ITIL configuration management process should determine that changes to the IT infrastructure have been recorded correctly, including relationships between CIs, and the configuration management process should monitor the status of the IT components to ensure that it has an accurate picture of the current version of these CIs.

As a first step here to establishing effective IT configuration processes, an enterprise needs to take an inventory of its existing IT resources. This exercise requires more than just surveying listings of installed software components and taking a physical inventory of the IT hardware on the floor. Exhibit 14.2 contains a list of the types of resources that should become CIs to define the configuration environment and as the building blocks for a CMDB, as discussed in the sections following. Effectively implemented, the inventory also should provide both management and the IT function with information and areas for further investigation in the following IT product policy areas:

- Which IT components are we currently using, how many different versions of each are in place, and how long have they been in use?

EXHIBIT 14.2 Examples of CMDB Configuration Items

- All physical computing platforms including desktop, laptop, rack-mounted servers, blade servers, and other stand-alone devices.
- All network devices and appliances, including network-connected printers.
- All application, middleware and software utilities, including end-user, management, and support products.
- All installed operating systems as well as software development package tools such as JAVA, C#, and SDLC management software tools.
- Operating system and network device patch installs.
- PBX and related telecommunications hardware and software.
- Installed business services or elements of these services.
- Documentation packages for applications, systems, and both policy and process standards.

- Which IT components can be potentially phased out and which require upgrading?
- What licenses are in place and are they adequate?
- How standardized is the overall IT infrastructure across the enterprise?

The idea here is that IT configuration management and CMS concepts should not just be IT function issues in an enterprise. A team of IT specialists including IT management and other key users of IT resources should be assembled to build and construct an enterprise CMS. Attention should be devoted to gaining CMS project team members from non-IT people in the enterprise who typically use other systems resources and have limited contact with the more centralized, corporate systems. An effective CMS has to include all of these information groups.

Gathering and Analyzing Configuration Management Requirements

While many managers and IT professionals understand the importance of having effective IT configuration processes in place for an enterprise, the process to specifically gather and define the requirements necessary to launch enterprise-wide configuration management can be a challenge. This exercise should start by looking at the configuration tools in place, updating them as required, and then making high-level configuration management connections, reducing these to more practical expectations and then moving to measurable requirements for an IT configuration process.

This process of building and launching IT configuration management components and defining their necessary requirements should normally start by planning, authorizing, and launching a formal IT systems development project, following the project management governance principles described in Chapter 16. Strong project management practices are important tools for launching an effective configuration management process. The IT configuration management project should include the following four elements:

1. **Define the IT configuration elements.** This step requires an overall definition of the configuration scope, a catalog or listing of the configuration items such as are shown in Exhibit 14.2, and a change tracking process to manage the CIs in the IT environment.
2. **Build IT configuration relationships.** These various identified CIs should be linked to IT and business processes.
3. **Optimize IT configuration processes.** The project team may find that various CIs are essentially duplicates of one another, but each is maintained in a different system or database. There should be a strong effort to simplify and implement these processes. For example, accounting system general ledger numbers should be maintained in only one repository. Keeping such a list in multiple locations will only lead to errors or other problems going forward.
4. **Develop consistent IT configuration management documentation processes.** This is an important governance standard that has been part of our discussions on IT governance in many of these chapters.

This whole configuration management process is similar to almost any that should be employed when there is a need to organize a large amount of often differing but related information elements with a need to be able to regularly reference them and to make changes as required. While personal records, such as an individual's income tax receipt records or a retail merchant's records of products and related repair parts, are often at least informally organized as configurations, many IT functions miss these types of implementations. They install new systems and software and often rely on the vendors to provide some level of revision control but do not have effective IT configuration management processes in place.

An enterprise IT function should take the necessary steps to implement configuration management as a key component of all IT operations. Such an effort may force IT to back away from some other regular projects, but an effective process will offer benefits for both IT and the users of IT services.

Steps to Implementing IT Configuration Management

An IT function should develop standards for its software and hardware versions. Version control is the practice of deploying consistent software versions on similar network devices. This improves the chance for validation and testing on the chosen software versions and greatly limits the number of software defects and interoperability issues found in the network. Limited software versions also reduce the risk of unexpected behavior with user interfaces, command or management output, upgrade behavior, and feature behavior. This makes the environment less complex and easier to support. Overall, software version control improves network availability and helps lower reactive support costs.

Version control for IT components is often easier said than done. Both enterprise IT operations and their software teams should define and determine device classifications based on their classifications, stability, and new feature requirements. In a larger multiunit enterprise, individual software versions should be installed for similar devices.

Standards can often slip here, where, for example, the west division of some enterprise may have forgotten to install some minor systems update that the east division put in place. While outputs may look about the same, matters can be forgotten until some future systems issue causes problems.

In order to establish effective IT configuration management controls, software specialists should test, validate, and pilot chosen software versions. Next steps include documenting successful versions as standards for similar-device classifications. The concept here is to consistently deploy or upgrade all similar devices to a standard software version.

An IT CMS is a key element of effective IT governance. We really cannot manage and control all of our IT resources until we have an understanding of how everything fits together. A key element of all of this is the need to establish standards and procedures throughout the total enterprise such that the enterprise IT function has a good understanding of all of the IT resources they have installed, they are all linked together, and they are used consistently across the enterprise. The effective implementation of ITIL, as discussed in Chapter 6, and service catalogs from Chapter 12 contribute to this environment. However, an important element in effective implantation of configuration management is the implementation of a CMDB, a central component and repository of IT configuration management processes.

THE CONFIGURATION MANAGEMENT DATABASE: AN OFTEN DIFFICULT CONCEPT

A configuration management database is a single database that contains all relevant information about the components of the information system used in an enterprise's IT services as well as the relationships between those components. A CMDB provides an organized view of data and a means of examining that data from any desired perspective. Within this context, components of that CMDB information system contain linked and referenced configuration items, as described in Exhibit 14.2. A CI can be any conceivable IT component, including software, hardware, documentation, and responsible personnel, as well as any combination of them. The processes of configuration management seek to specify, control, and track configuration items and any changes made to them in a comprehensive and systematic fashion.

Several major software vendors offer CMDB software products. Exhibit 14.3 provides a conceptual view of what such a database should look like or its major components. The objective of this chapter is not to provide a technical description of how to select and build a CMDB but to describe its major components. Based on Exhibit 14.3, a CMDB should consist of the following elements or components:

- **CMDB user administration.** As a major database controlling enterprise activity, there is a need for a user interface and administration function. This would be a combination of IT technical resources to help with managing and monitoring the overall database as well as administrative processes to define and input new CIs as systems and processes grow and change. In addition to building CIs, there are needs for tools to query their status and to optimize performance.

- **CMDB security and user access tools.** While there is always a need for IT security and access control tools, the issue becomes even more important with a thorough, comprehensive CMDB. This is an area where someone could gain access to all enterprise data resources, and strong security controls are essential.
- **Database configuration management facilities.** This is a database specialty area tool that should be available to model the CI-based data structures to promote CMDB efficiency. Most important, this is an area where strong revision control facilities must be in place.
- **Data management and the database repository.** This element describes the actual physical database, its operating software, and the physical and environment controls. Skilled software database specialists are needed here to manage and tune the software. Of course, proper backup and continuity processes must be in place.
- **Security and data protection controls.** Just as there are needs for strong security and access controls to be in place over the user interface links, these security processes are even more important as they serve as repositories from the CMDB and the other using systems.
- **Data integration repositories.** A fully functioning CMDB should provide links to a wide range of other systems and processes. This is the important output link between the CMDB and the large body of other applications.
- **External discovery and monitoring tools.** Going beyond the actual enterprise CMDB, there should be a wide variety of others who have a need to access and monitor the CMDB data. Examples could be IT auditors with a need to review certain data structures, other processes that are not regular CMDB users, and even regulatory officials.
- **Other data repositories.** Exhibit 14.1 illustrated that a CMDB is usually not the one and only centralized repository of configuration data, but there will be other configuration database tools as well. For this or any other CMDB repository, linkage to these other interfaces should be in place.

The previous list describes the attributes of a CMDB. For a large and complex enterprise, it is a challenging task to launch and effectively implement such an IT tool and process, but there should be ongoing benefits from systems efficiencies. The implementation of an effective CMDB is an important IT efficiency and governance tool for any enterprise with a relatively complex set of IT systems and processes.

ESTABLISHING AN ENTERPRISE CMDB

Multiple software vendors advertise CMDB products as part of their offerings. Although most should follow ITIL standards, there is no consistent definition among them. While a CMDB implementation can be a major project for an enterprise, a smaller and less mature IT organization does not need to invest in expensive and complicated CMDB software. It can implement a limited set of configuration management processes through the use of basic office tools like Excel. A CMDB is a system for managing knowledge more than it is a product, and it is more of an index than a complex database. That is, as long

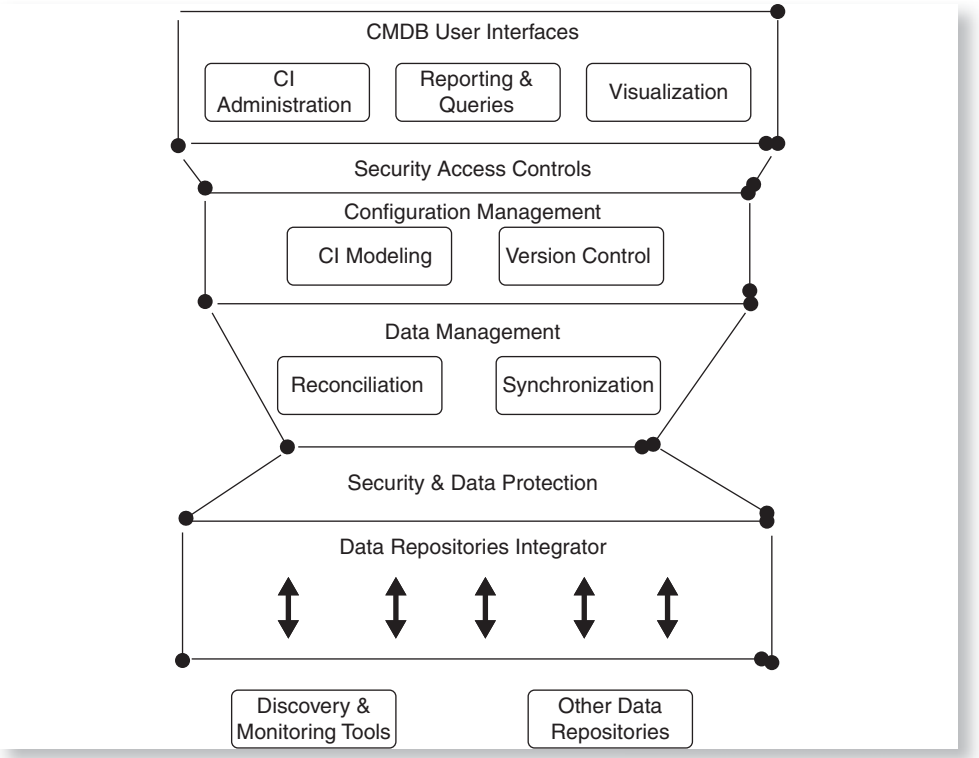

EXHIBIT 14.3 CMDB Conceptual View

as the amount of CI data is small, an enterprise can get the benefits of a CMDB in any number of ways—paper, Visio diagrams, Access databases, people's heads, and so on. This is exactly what has been installed in many enterprises.

However, when an enterprise IT organization spans large geographies with hundreds or thousands of users and locations, the sheer number of these configuration variations requires a specialized CMDB solution. IT or the management team that is searching or installing an appropriate solution should establish standards and performance requirements for their CMDB. An enterprise CMDB requires some unique features. First, a true enterprise CMDB solution is based on an old database concept called dimensional modeling that is a bit out of style. An enterprise CMDB solution has to be based on a dimensional database rather than the relational database model that is common today. Today's relational databases, such as Oracle or IBM's DB2, simply cannot do the job for a CMDB.

These concepts of relational versus dimensional database models go back to the 1970s with many of the issues long forgotten by most of us who were around then. In this section, we will explain what an enterprise-class CMDB software solution requires: a dimensional database, federation, reconciliation, synchronization, and data modeling. Our objective here is not to provide a treatise on database modeling but to outline some key concepts necessary for an effective enterprise CMDB.

Relational vs. Dimensional Database Architecture

A relational database uses a "row-and-column" approach similar to the way data is stored in Excel spreadsheets or in an online transaction processing system. Data stored in a relational database is easy to look up when you know in advance what you want to see. However, a CMDB does not store most of its data; it references data stored externally in other, perhaps relational, databases. A CMDB also is used to provide what is called contextual awareness over not obviously related bits of data.

For example, a common inquiry posed to the CMDB might be, "How many users, in sales, used the SAP system during the last week of the month?" This kind of query is not well suited to a centralized relational database with prebuilt query transactions. There are just too many possible combinations of data. This type of query has to pull information from many systems, and the data it needs is probably not all nicely lined up in rows and columns ready to query. Rather, an enterprise CMDB should use a dimensional technology that represents data as different dimensions or planes.

The dimensions of a CMDB often include local (e.g., city, state, floor, etc.), work groups like sales, marketing functions, and so on, IT services like SAP or e-mail, date ranges, and others. Instead of an Excel spreadsheet with rows and columns, one should think about a Rubik's Cube type of data representation to begin to get the idea. The logic required is not new—it has been around for years in the form of what we call online analytical processing (OLAP). However, a simple OLAP does not give you a CMDB, for a couple of very special reasons. First, most CMDB data resides outside of the CMDB system. In order to pull this data from many sources requires federation—a new CMDB buzzword, discussed in the sections following.

Database Federation

A CMDB is what is called a metadatabase; that is, it is a database that references other databases. A major requirement for a CMDB is called dimensional modeling or federation, the referencing of data from several sources. An issue that drove data federation the first time around was data validity. If you make a copy of something, then what is definitive? The original or the copy? And how do you know if the copy is the same as the original?

The concepts around CMDB federation are how to connect to heterogeneous data sources, resolve which bits of data are definitive, and then create and store keys with unique data not found in any external data source but still required. For example, data not found in any of these systems might be the name of the IT service and which workers use it. There also has to be a method to store the awareness of the types of data to be found in each federated data source in order to process ad hoc queries.

The idea of CMDB federation requires "connecting to multiple data sources," but having a CMDB system that can actually federate these data sources. This is a very tall order indeed, and federation is just one of these four equally complicated CMDB technical requirements. Consider this: What if two data stores reference the same data? Which data store is definitive, then, and more importantly, how would you determine which is definitive? This is the issue of data confrontation and reconciliation.

CMDB Reconciliation

Aside from the issue of simply connecting to heterogeneous and possibly competitive data sources, a big problem with federation for a CMDB is called data confrontation. During the creation and maintenance of the contextual information in the CMDB metadatabase, key bits of data transfer from federated data sources to the CMDB data store. Since it is common to have multiple applications and systems that overlap and monitor the same IT assets or store similar data, possible data inconsistencies and redundancies arise: This is data confrontation.

Reconciliation implies adjusting data derived from more than one source to eliminate duplicates and maintain consistency. Federation is useless with reconciliation. Reconciliation, however, is not the end of the requirements for an enterprise CMDB. Adding even more complexity to a CMDB system is the need to handle any changes arising from successful reconciliation, and this leads to synchronization.

CMDB Data Synchronization

Data stored in a federated CMDB can change when such occurrences as the name of the project manager (e.g., the "user") changes, or the type of hardware changes from, for example, Cisco series 2504 software to Cisco 2801. Reconciliation has to be able to resolve these differences to maintain the integrity of the CMDB. But this is IT, not "simple" data warehousing. No CI represented in an ITIL-aligned CMDB should change without a request for change. Thus a CMDB system that can successfully federate and reconcile data must also be able to alert when it detects unauthorized/unplanned changes. Failure to synchronize reconciled changes will quickly result in an out-of-control CMDB—a recipe for disaster.

This means that a CMDB system requires an awareness of approved changes. Then, when the reconciliation engine detects and resolves a change in infrastructure or data, it has to compare this change to an expected list of approved changes and generate an alert if the change is unapproved (e.g., not planned). This alert brings CMDB data to the attention of its administrators, who need help visualizing, mapping, and displaying data—the next major technical requirement of modeling.

CMDB Modeling

Modeling is the mapping and visualizing of synthesized database relationships that are IT service definitions and CI interconnections. Modeling is more than reporting or displaying lists of resource trees and forks. The CMDB has to be able to visibly display its data in ways that let humans use the information in impact assessments for change management, privilege determination at the IT function's service desk, troubleshooting through incident or problem management processes, and dozens of other ad hoc inquiries from all over IT operations.

This modeling requirement goes way beyond the simple "directory tree" listings commonly found in some CMDB products. Federation, reconciliation, and synchronization are worthless if users in IT cannot get definitive, understandable answers to their complex questions quickly. This often requires representing complex relationships between CIs graphically, on demand.

In summary, an enterprise CMDB is not a singular database but a complex system that has to federate other data stores, reconcile alternative views of the same data, detect unauthorized changes, synchronize approved changes with its own metadata store, and be able to dynamically represent configurations graphically on demand. This is no small task.

An enterprise developing its own CMDB should keep these concepts of multidimensional modeling and the issues of federation, reconciliation, synchronization, and modeling in clear view. While the senior manager who is assessing an enterprise's CMDB plans or installed systems may not have a computer science level of understanding of these concepts, it is fully appropriate for a senior manager to ask his or her IT resources how they handle these issues. If one is uncomfortable with the answers, it may be necessary to work with a consultant on these issues.

In all cases, an enterprise launching a CMDB should create processes to monitor and ensure that federation, reconciliation, synchronization, and modeling occur. Failure to manage these critical issues can quickly convert a CMDB project from an asset to a liability.

IT PORTFOLIO MANAGEMENT

IT management and the users of these systems and processes have typically implemented large numbers of systems and processes over time that are directly or loosely connected with other systems or exist as stand-alones. IT managers have typically been designated as responsible for some of these, while IT user functions may take direct responsibility for others. Often each responsible manager thinks his or her systems are the most important when there are scheduling conflicts, update needs, or other system needs. An IT organization can typically realize some massive service and investment savings if it looks at these often disparate IT systems and processes and manages them as portfolios of IT resources.

IT portfolio management is the division, reclassification, and application of management of large classes of IT resources. Examples of IT portfolios might be planned systems initiatives, major new IT projects, and ongoing IT application support services.

The promise of IT portfolio management is the quantification of previously informal IT efforts, enabling measurement and objective evaluation of investment scenarios. The concept of IT portfolio management is similar to financial portfolio management, but there are significant differences. Financial portfolio assets typically have consistent measurement information criteria such as returns on investment. On the other hand, IT value measurement often requires considerable effort. The problem is that IT investments are not liquid, like stocks and bonds, and are too often measured using only nonfinancial yardsticks. In addition, assets in an IT portfolio have a functional relationship to the organization, such as an inventory management system for logistics or a human resources system for tracking employees' time. Because of their importance to the enterprise, it is difficult to measure them as some form of IT portfolio.

IT portfolio management provides advantages over IT investment approaches and methods. Other benefits include the central oversight of budget, risk management,

strategic alignment of IT investments, systems utilization demand, and investment management, along with standardization of investment procedures, rules, and plans.

Implementing IT Portfolio Management

IT management, with the agreement of other key systems users, should develop a portfolio management approach for managing its IT resources and developing overall goals and performance objectives from them. IT portfolio management is distinct from IT financial management in that it has an explicitly directive, strategic goal in determining what to continue investing in versus what to divest from.

For many enterprises, IT portfolio management is accomplished through dividing up its systems resources into three broad portfolio areas with subportfolios in each group:

1. **Application portfolios.** This can include all production applications. These can also be divided into subportfolios for different application groups, such as finance, manufacturing production, and engineering product development. The idea is to match and manage portfolios that have similar concepts and objectives, such as a portfolio including payroll-related applications, human resources systems, and employee training applications.

   Application portfolios should be based on established systems, such as headquarters office–based, field unit and international, and end user–controlled. These portfolios should all be based upon their relative value to the enterprise. Comparisons and assessments also can be based upon the level of contribution in terms of an IT investment's profitability. Additionally, this comparison can also be based upon such nontangible factors as the IT organization's level of experience with a certain technology, its users' familiarity with the applications and infrastructure, and external forces such as the emergence of new technologies and the obsolescence of old ones.
2. **Infrastructure portfolios.** These types of portfolios focus on the enterprise's information technology and infrastructure management software processes. Infrastructure management is sometimes divided into the categories of systems management, network management, security, and storage management software. The ability of enterprises to exploit IT infrastructure, operations, and management sourcing/service solutions not only depends on the availability, cost, and effectiveness of applications and services but also aids IT management in coming to terms with solution providers for managing the entire sourcing process. In their rush to reduce costs, increase IT quality, and increase enterprise competitiveness by way of selective IT sourcing and services, many enterprises and their IT functions do not consider the management side of the equation. The predictable result of this neglect is often overpayments, cost overruns, unmet expectations, and outright failure.

   Portfolio management of IT infrastructure software systems helps software specialists to make some hard decisions. For example, do we really want to upgrade to a new version of one of our databases? If so, how does that database application interact with similar database processes throughout the enterprise? What are the

overall costs to the enterprise in using this product and what values does the enterprise receive from it?

3. **Project portfolios.** Portfolio management should address such issues as spending on the development of innovative capabilities in terms of potential return on investment (ROI), reducing investment overlaps in situations where reorganization or acquisition occurs, or complying with legal or regulatory mandates. The management issues with project-oriented portfolio management can be judged by criteria such as ROI, strategic alignment, data cleanliness, maintenance savings, suitability of resulting solution, and the relative value of new investments to replace these projects.

   Many enterprises have practiced portfolio management over their various IT and operational projects through the establishment of project management offices. Project and program management processes are discussed in Chapter 16.

Portfolio Metrics: Achieving Value through IT Portfolio Management

Dividing up one's IT applications and other resources into separate portfolios is of little value to the enterprise unless some measures are established to assess their value and to help make other IT portfolio decisions. We should keep in mind that an IT portfolio is a group of related initiatives, projects, and/or programs that attain wide-reaching benefits and impact.

Although we have established a series of diverse IT portfolios, appropriate management groups should develop an ongoing mission for each of these various IT portfolios. One might have a goal of promoting the growth of business in certain areas covered by a group of applications by $X billion, while another might seek a measurable increase in customer satisfaction and another might seek increased enterprise revenues from new product developments.

A next step is to build strategies for meeting each of these portfolio goals and then to establish measures for their success. The whole concept is to look at various IT applications and resources in terms of how much they are contributing to the value of overall enterprise operations. Of course, when a portfolio is failing to meet its hoped-for mission and goals, it may be time to make some changes. This might involve retooling the portfolio components, totally changing approaches, or bringing new people into the mix.

IT portfolio management processes as well as strong configuration management systems should improve overall IT performance and improve IT governance operations. Both of these areas should encourage both IT personnel and general management to better think of IT operations as an enterprise business venture.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER FIFTEEN

Application Systems Implementations and IT Governance

THE APPLICATION SYSTEMS DEVELOPMENT PROCESS was once a major concern for IT organizations. That was the time when most IT programming and systems development functions designed their own new systems, coded the programs using IT department resources, and implemented and then tested the major program components of new applications. This development process sometimes led to a hall of horrors for some enterprises. The new homegrown IT applications frequently were delivered much later than promised, were poorly tested, and did not meet their stated objectives. Even worse, sometimes new application projects were launched with no clear understanding of the system's objectives. This era of failed application development projects goes back to the early days of IT, when everyone felt their own IT systems needs were unique and they had to develop their own applications to support those "unique" needs.

While dating himself to admit it, this author once worked in IT shops where there were systems development efforts to develop *new* accounts payable applications—effectively a check-writing application then—or even to develop and program new payroll systems! Given state and national rules, there are really few differences between the requirements of one payroll system versus another. However, back then there were few commercially developed applications to lease or purchase. Today, we generally buy this sort of software from an outside vendor who supplies and updates the software on the enterprise office client–server computer system or makes it available through a cloud computing environment (see Chapter 9 on cloud computing).

Despite the move today from in-house developed applications to a greater emphasis on vendor-supplied purchased software, there is still a need for an enterprise to develop, build, and test some of its own application systems or to custom modify purchased applications. This is particularly true when an enterprise today implements one of the complex multifunction and linked databases known as enterprise resource

planning (ERP) systems. These complex vendor-supplied systems have the ability to link virtually all application functions on one set of interlinked databases. For example, when an ERP system is installed in a manufacturing system's environment, an order for a product can update manufacturing and production systems, place a supplier order if additional materials are needed, and otherwise complete production sales and shipment processes.

As a key element of good IT governance processes, an enterprise needs to have strong IT systems development processes in place, whether building applications in a more traditional manner or licensing from a vendor for a cloud implementation.

This chapter discusses the IT governance aspects of IT application development approaches from the perspective of applications developed through well-recognized systems development processes, to the common rapid application development processes using report generator types of applications, to comprehensive ERP databases. Enterprise management should have a good understanding of the IT governance processes surrounding its new systems applications development efforts.

THE SYSTEMS DEVELOPMENT LIFE CYCLE: A BASIC APPLICATION DEVELOPMENT TECHNIQUE

The very early years of IT applications development were filled with new systems disasters in many enterprises. Typically, a senior manager—often the organization's financial controller—would tell the head of IT that he wanted a new application to fulfill some need. Without too much further analysis, a programming team would then be assembled to write programs to meet that need. The results were often failures. The new application, if it worked and was delivered in any reasonable period of time, often did not meet management requirements and expectations. We are talking about the early days of IT mainframe systems here when purchased software was unknown and everyone wrote their own applications.

IT governance concepts were certainly unknown in those early days of mainframe systems, COBOL programs, and primarily batch-oriented systems, but there certainly were a lot of application development failures. To place some order in this systems development process, the major hardware and software vendor in those days, IBM, launched a systems development methodology known as the systems development life cycle (SDLC). Although many others have developed variations of the approach, the SDLC approach has become a key process to develop effective IT applications.

Exhibit 15.1 shows the key SDLC action steps in a circular or continuous process. Although an enterprise and its IT function can start a new systems development process at any point, there is first a need for a requirements analysis process. That is, before an IT shop starts any systems project effort, it should obtain a formal understanding of the objectives and expectations of the new system project. This is normally documented and approved by a management process with estimates of the costs and expected benefits of the new application.

Once the new application has been approved, it should move to a formal application design and programming phase. Each of the new system's programs and components

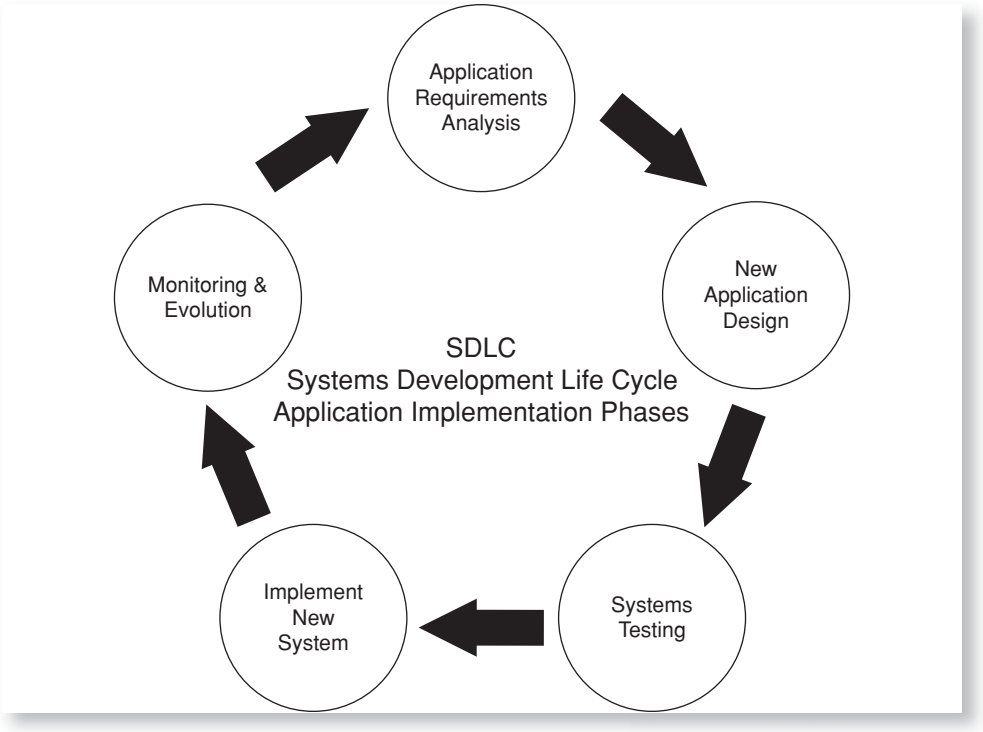

EXHIBIT 15.1 Systems Development Life Cycle (SDLC) Phases

should be developed, documented, and then unit tested. We then move to a total systems testing and implementation phase, leading to the system implementation.

The whole concept behind the SDLC process is that once we have implemented the new application, IT and enterprise management should be monitoring its success and progress. This may lead to a need for system revisions or a totally new application. Thus the SDLC is a continuous improvement process for development and ongoing monitoring of new IT applications. Historically, it went back to mainframe and batch systems and required detailed approvals and documentation of each process step.

Even though we now have moved to rapid development, and prototyping application development processes largely rely on vendor-supplied software, these basic SDLC elements should be in place for any IT new applications development process. That is, new systems applications should always go through some formal system requirements analysis, formal application launches, and processes to improve and retire them in their later lives.

Depending upon the type and nature of the IT application system development, a requirements analysis can be either informal or quite formal, but Exhibit 15.2 outlines the contents of a typical systems development requirements analysis. The whole key to such a process is that a project team should take a hard look at user or even IT management requests for a new application and determine whether they seem to make sense. Properly done, many IT application requests are dropped after the initial analysis. However, the requirements provide a formal mechanism to review new application requests and determine if they seem to make sense.

A requirements analysis is only one step in the SDLC cycle, but it should almost always be included in the systems development process. As a key component in the IT governance process, an enterprise and its IT function should have some form of SDLC process in place, even though they are using rapid development processes, such as prototyping, discussed in the paragraphs following.

IT RAPID DEVELOPMENT PROCESSES: PROTOTYPING

The use of formal SDLC processes made a lot of sense in the earlier days of IT systems, when enterprises fully developed and programmed their own applications and when there was a need to document and formalize new application development processes. A variety of vendors sold development approaches to businesses and their IT functions. The products marketed at that time asked systems developers to prepare detailed documentation covering all phases of their efforts. Properly followed, these methodologies would have resulted in well-documented and well-planned new application systems. Their objective was to improve the process of developing and implementing new IT applications. The only problem was that extensive documentation development methodologies often did not work. The published methodologies required the completion of many formal documents, all requiring reviews and approvals. However, IT and management looked at these new development efforts and continually decided things were not quite right and looked for ongoing, often minor changes and revisions.

The vendors of those published formal SDLC methodologies have essentially gone away, just as we have gone away from those formal mainframe systems. New

EXHIBIT 15.2 Systems Development Requirements Analysis Process

- **Prepare for Systems Requirements Analysis**. Assign project team members and gather background information, including requesting and other potential user groups, to allow for the capture and analysis of system requirements.
- **Determine Business Requirements**. Identify both in-scope and out-of-scope requirements and define and document planned business rules as well as potential interfaces to and from the new application.
- **Define Process Model**. Define and diagram the major business processes that will interact with the proposed new application and decompose these into manageable functions and subfunctions until no further breakdown is feasible.
- **Define Logical Data Model**. Understand and logically model the data that supports the proposed application and identify the application's entities and their relationships to other entities as well as defining attributes along with their business attributes.
- **Reconcile Business Requirements with Model**. The project team should ensure that the defined process and logical data models accommodate all requirements and business rules.
- **Produce Functional Specifications**. The interfaces, processes, and data should be merged to systematically describe how the proposed user will use the application and how the associated data will be retrieved, processed, and stored.

applications today are often built with easy-to-use table-driven software tools. We build an initial or prototype version, modify that prototype to fine-tune requirements, and then implement the application. These types of applications are developed through a process called rapid application development (RAD), a software development methodology that uses minimal initial planning and prototype approaches where a rough initial version is launched and then adjusted and modified until all are pleased. Users and IT look at the prototype version and make further changes to eventually come up with the final application. This lack of extensive preplanning generally allows software to be written much faster and makes it easier to change requirements. A simplified version of this RAD software development process is shown in Exhibit 15.3.

The RAD process starts with the development of preliminary data and business process models to define preliminary requirements. Using one of the powerful report generator software tools available today, a sample or prototype version of the application can be created. The prototype model is then verified against the requirements to refine the data and process models. These stages are repeated iteratively; further development results in a combined business requirements and technical design statement to be used for constructing new systems.

RAD approaches often entail compromises in functionality and performance in exchange for enabling faster development and facilitating application maintenance. The RAD systems process consists of the following four phases:

1. **RAD requirements planning phase.** Enterprise IT should use some of the same elements found in the systems planning and systems analysis phases of a traditional SDLC process as outlined in Exhibit 15.2. However, under RAD, the users, managers, and IT staff members discuss and agree on business needs, project scope, constraints, and system requirements. This phase ends when the team agrees on the key issues and obtains management authorization to continue.

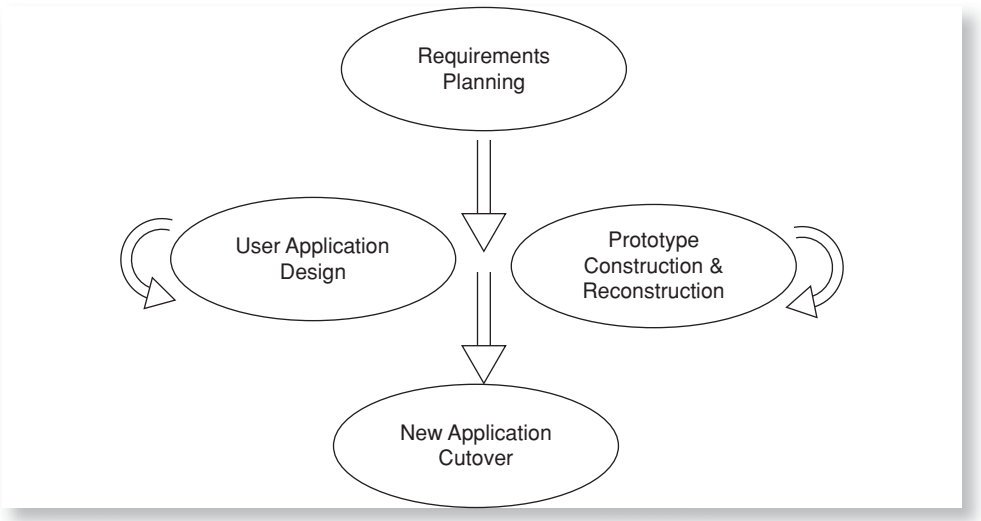

EXHIBIT 15.3 Rapid Application Development (RAD) Software Development Process

2. **RAD user design phase.** Here, users interact with systems analysts and develop models and prototypes that represent all system processes, inputs, and outputs. The RAD groups or subgroups will typically use IT department application development tools to translate user needs into working models. This user design phase is a continuous interactive process that allows users to understand, modify, and eventually approve a working model of the system that meets their needs.
3. **Construction phase.** This RAD phase focuses on program and application development tasks similar to the SDLC. In RAD, however, users continue to participate and can still suggest changes or improvements as actual screens or reports are developed. Its tasks are programming and application development, coding, unit integration, and system testing.
4. **RAD cutover phase.** This final phase resembles the final tasks in a SDLC implementation, including data conversion, testing, changeover to the new system, and user training. Compared with traditional methods, the entire process is compressed. As a result, the new system is built, delivered, and placed in operation much sooner. Its tasks are data conversion, full-scale testing, system changeover, and user training.

The RAD systems development approach was initiated at about the time that enterprises and their IT functions began the transition from classic mainframes to client–server systems, during the growing predominance of desktop and laptop systems and most significantly the Internet. Going back to the mainframe SDLC days, many enterprise IT users had expressed frustration with the slow development processes, new-system failures, missed budgets, and a host of other problems. The introduction of RAD tools to these systems users was almost a revelation. They could get a quick look at prototype versions of systems reports and even processes and then could move forward with the quick-and-dirty RAD version.

Because of its ease of use, enterprises that encourage the use of installed RAD tools can find themselves in some security and application internal control problems if they embark on too aggressive of a RAD new applications approach without installing adequate controls in new applications. Exhibit 15.4 outlines some IT governance controls and procedures that should be put in place surrounding the use of RAD processes.

Many enterprises today are developing their own customized reports to support purchased software applications. Purchased software applications today almost always are developed using a report generator or RAD facility for that software. The IT governance best practices discussed in this chapter apply for all of these tools.

ENTERPRISE RESOURCE PLANNING AND IT GOVERNANCE PROCESSES

Typically employing a comprehensive database as an information repository, ERP systems integrate internal and external management information across an entire enterprise, embracing their finance/accounting, manufacturing when appropriate, sales

EXHIBIT 15.4 IT Governance RAD Controls and Procedures

Rapid application development (RAD) is a software development technique that emphasizes short development times (30–90 days). The technique is inappropriate for developing complex applications or applications that quickly process significant volumes of transactions, such as batch processing environments. An enterprise may appropriately use the technique to develop or redesign lower-risk applications, or less complex applications such as transactional Web sites that do not involve a high degree of throughput. Additionally, depending on an enterprise's risk tolerance and the mission-critical designation of an application, an enterprise should use IT governance controls and procedures to ensure that appropriate RAD techniques are employed during the IT new application design and development phases within a structured development methodology. The following outlines some general good IT governance RAD controls and procedures:

- Select an appropriate application report generator tool that is flexible and meets business application needs. Management should ensure that the development technique selected is appropriate for managing the complexity and risks of the applications being developed.
- Establish enterprise IT rules such that only the approved RAD will be used for production application purposes unless there has been specific approval by IT senior management.
- Implement initial and ongoing training for IT and appropriate users on the use of the selected RAD software tool.
- Establish IT function standards for applications developed through RAD processes involving the formal phases of initiation, development, and implementation. The short duration of RAD projects necessitates the quick identification of functional requirements, which should remain largely unchanged during the development process.
- Determine that appropriate levels of IT professionals and end users are assigned to RAD projects to construct and modify designs. For larger RAD projects, specialists such as database administrators, network technicians, and system programmers should be assigned for key RAD decisions.
- Appropriate enterprise RAD standards and controls should be in place to ensure:
    - Organizations use RAD techniques only when appropriate.
    - Management includes adequate security and control features in all developed applications.
    - Quality assurance personnel verify that security and control features (commensurate with risk levels) exist and function as intended.
    - End users are appropriately involved throughout RAD projects.
    - Project managers closely monitor project activities.
- Determine that all RAD applications are appropriately documented and done in parallel with the development of the application. With the simultaneous production of documentation, without aggravating the application's developmental time, RAD applications will save time during the future maintenance of the system.
- Establish strict principles in the naming/coding rules, so that one RAD developer almost always understands the application generator script source code generated by another RAD professional or IT professional.

and service, customer relationship management, and so on. ERP systems are complex databases that automate this activity through an integrated software application. Their purpose is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders. The goal of ERP is to improve and streamline internal business processes, which typically requires reengineering of current business processes.

We can think of the functions of an ERP system through the process of manufacturing where some product part needs to be designed, resources ordered to build the part, part costing and marketing processes established for the part, material orders placed, and production started, and then the entire stream of production and operational processes for receiving a customer order, shipping, and billing for the item. These processes and others involve a series of separate but interrelated activities that were once managed by a series of separate IT applications such as receiving, inventory control, production scheduling, shipping, accounts receivable, and more. An ERP system ties together all of these activities and more into a tightly linked series of database functions.

An ERP system attempts to integrate all departments and functions across a company onto a single computer system that can serve all its different departments' particular needs. This can be a tall order to build a single software program that serves the needs of people in finance as well as the people in human resources and in the warehouse. Prior to ERP, each of those departments typically would have its own computer system optimized for the particular ways that the department does its work. But ERP combines them all together into a single, integrated software system that runs off a single database, allowing the various departments to easily share information and communicate with each other. That integrated approach can have a tremendous payback if companies install the software correctly.

There are many ways to describe an ERP system, but Exhibit 15.5 shows basic accounting data flows for an enterprise business, including purchase orders, accounts payable, and other typical business systems processes that would be part of an ERP system. These are the elements of the systems requirements to build a manufacturing part, described previously, and were traditionally separate systems processes with key data and transaction files for each as well as links to other key applications, such as the

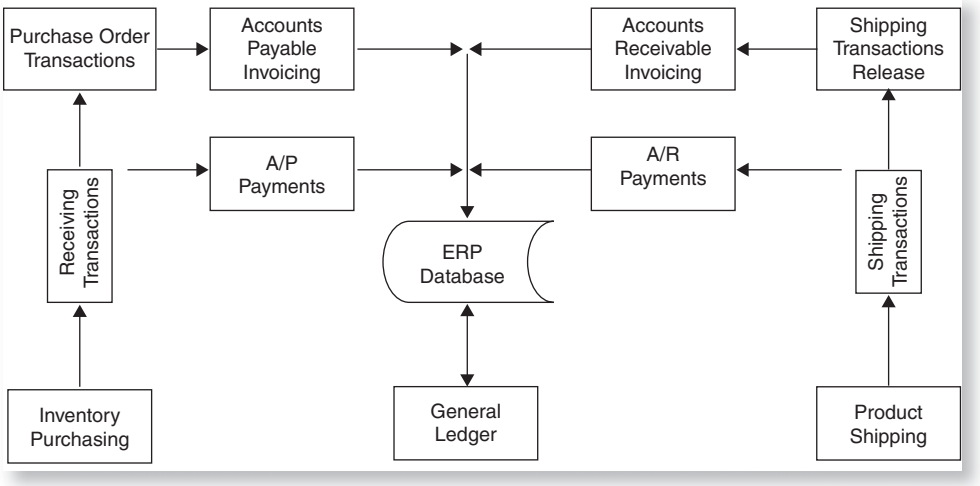

EXHIBIT 15.5 ERP System Example Configuration

general ledger system. While this exhibit shows a series of manufacturing distribution processes, such as traditional accounts receivable and accounts payable functions, a complete ERP application for an enterprise would include a much larger array of systems, such as marketing and human resources. They would all be tied together through common data descriptions and links.

The senior manager might wonder why it takes so long to get customer complaint data from the product returns system. Other staff members may grouse that they have to reenter similar transactions into different but related applications. A common combined database—an ERP system—often appears to be the easy solution. However, the implementation of an ERP system into an enterprise is no small step. Even with the best of conditions, such a system will take considerable amounts of enterprise time and resources, with the active participation of key managers, IT staff, and even other stakeholders who have interests or concerns.

From an IT governance perspective, there are some key points to consider when implementing an ERP database for an enterprise:

- **Define ERP objectives and requirements.** This is a relatively new IT systems concept; there is much published hype about what a comprehensive ERP database might accomplish. However, based on their knowledge of what a comprehensive ERP database might accomplish, project initiators should develop strong objectives and requirements for a new ERP implementation project.
- **Build a cross-functional project team.** An ERP database is more than just a new IT system but will involve many members of an enterprise. A cross-functional team of IT and members of the user community should be appointed to lead the upcoming ERP project.
- **Recognize the costs and time requirements to implement ERP.** For a single-unit enterprise with 25 to 1,000 employees, a smaller ERP database software package can cost up to $250,000, while for a larger multi-unit enterprise with up to 5,000 users, the basic ERP software may cost up to $2 million. An enterprise should develop realistic expectations of the time requirements for this level of project and assume that such a major IT project will require at least one year.
- **Select an ERP software product.** There are a large number of vendors offering ERP software, with major providers such as SAP, Oracle, and Microsoft, as well as less familiar vendors such as Epicor. To avoid an endless stream of vendor meetings and glossy promotional materials, the selections team should stand firm on their defined requirements and budget objectives as well as the enterprise's current software environment. Any viable ERP software vendor should be able to supply a representative test version of their ERP product.
- **Apply formal project management techniques to the ERP implementation.** Chapter 16 outlines formal project and program planning techniques. Since an ERP is a major undertaking, an enterprise should develop and follow formal project planning methodologies for a major ERP endeavor.
- **Establish a test database for the ERP and begin phased implementation.** Once it is up and running, the enterprise ERP application will impact a large number

of regular applications. However, care should be given to launching a phased implementation on an application-by-application basis, using the test database in the earlier stages of the project.

- **Provide extensive user training.** The new ERP application may involve new transaction formats and other sometimes small but subtle systems changes. As part of the project plan and as a responsibility for the ERP implementation team members, there should be a strong user training program.
- **Establish project budgets and closely monitor ERP system costs.** Beyond the license fees for the selected database software, an ERP project can be an expensive undertaking for an enterprise. Project team members as well as others involved with the effort should be required to log their hours as well as charging any direct expenses to the ERP project. These charged expenses should be closely monitored and questioned when appropriate, however. As a really fundamental IT governance concern, it can sometimes be a problem when staff members charge their hours to a project even though they are not really performing direct project activities.
- **Establish an exit strategy, if necessary.** A well-planned and well-executed ERP implementation can yield some major tangible and intangible advantages to an enterprise, but things can sometimes go wrong. For example, some of the ERP database vendor's software features may not quite work as promised or expected, there may be technical problems with systems interfaces, or any of a host of other potential problems. As the old expression goes, rather than throwing good money after bad, the ERP team should develop an exit strategy to gracefully end project efforts and return to normal IT and business operations.

EXHIBIT 15.6 Tangible and Intangible Benefits from Enterprise ERP Implementations

Tangible ERP Benefits

- Inventory Reductions
- Personnel Reductions
- Order Management Improvements
- Streamlined Linkages
- Financial Close Cycle Improvements
- IT Cost Reduction
- Procurement Cost Reductions
- Cash Management Improvements
- IT and Systems Maintenance Reductions
- Improved Systems On-Time Delivery

Intangible ERP Benefits

- Greater Access to and Visibility of Systems Information
- New Improved Processes
- Greater Customer Responsiveness
- Systems and Process Standardizations
- Improvements in the Supply Demand Chain

Despite the previous cautionary comments, a successful ERP implementation can bring some strong tangible and intangible benefits to an enterprise, as outlined in Exhibit 15.6. An ERP implementation can be a major project for an enterprise that can yield many benefits. Just as we have discussed the importance of strong IT governance processes in SDLC processes as well as for RAD work, these issues are extremely important when launching an ERP database for an enterprise.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER SIXTEEN

IT Governance Issues: Project and Program Management

WHILE ENTERPRISES MANAGE MOST OF THEIR ACTIVITIES through formal organization chart structures, a significant group of enterprise activities are organized and managed as projects. A term that is used in science, governmental, or even in school activities, a *project* is a collaborative activity within an enterprise, involving such activities as research or IT development. Projects are specially planned to achieve a particular aim, and contrasted with enterprise regular activities, projects are usually defined as having a temporary rather than permanent organizational structure. They are constituted by teams within or across organizations to accomplish particular tasks under time constraints.

Many IT systems development efforts are organized and managed as projects, and when an enterprise or its IT function is faced with managing a series of similar but different projects, those groupings are called *programs*. Projects and programs are often effective ways to manage and implement IT systems and process changes, but they also can cause some governance and control problems since they are efforts that typically cross regular organizational boundaries and require special monitoring and project control mechanisms.

This chapter will consider effective project and program management techniques with an objective of improving overall IT governance. We will introduce the *Project Management Book of Knowledge* (PMBOK) standards issued by the Project Management Institute (PMI; www.pmi.org) and will discuss why compliance with these standards is important for effective project and program management.

THE PROJECT MANAGEMENT PROCESS

In many enterprise IT and other business operations today, the term *project* is too often used rather loosely. IT application developers or people in other areas of the enterprise

have often been asked to organize a "project" to implement some special effort, and the organization and planning efforts for such a "project" have meant different things to different people. Those efforts often involved a designated lead person calling the assigned project team together and doing little more than saying, "I want you, you, and you" to perform various project tasks. Little thought was given to the project's organization or necessary planning steps. These informal "project" efforts often failed because the assigned team did not understand its individual as well as the overall project objectives; in addition, neither the project's time requirements nor scope were defined. In many instances, these efforts resulted in project failures because of time and budget overruns, or for many other reasons. Often that failure was due to the lack of a consistent structured project management approach.

Project management continued to be just a poorly defined concept until the mid-1990s. While there were good methods in place for such infrastructure projects for building a highway bridge, this was an era when there were many IT systems development project failures. With the exception of some U.S. government–led approaches to improve these IT development projects, there was no consistent approach to project management over many years. Matters changed when the Project Management Institute (PMI) was launched. Started by a small group of U.S. professionals looking for a more consistent definition of their work, as of 2012, PMI is an international professional organization with about 600,000 members and credential holders in 185 countries. PMI has researched, developed, and published a wide range of project management guidance materials. Its most significant publication is a standards-like document called the *Project Management Book of Knowledge* (PMBOK),[1] a comprehensive guide to all aspects of the project management process. PMBOK has become the worldwide professional standard for project management practices.

Exhibit 16.1 shows PMBOK's definition of a project. Although this guidance is rather lengthy and perhaps too general and comprehensive for just IT governance guidance, it defines the concept of a project as a temporary endeavor with a definite beginning and end date and with specific goals or objectives. Projects often cross regular organization lines and operate somewhat separate from or outside of normal organization or enterprise procedures. A project may be staffed with people from several enterprise organizational units, reporting on a dotted-line basis to an independent project manager. In some instances, these project team members may have only part-time responsibilities for the project but will still have some of their regular job responsibilities. Because project activities often cross organizational lines and operate as separate individual efforts, IT governance issues can be a problem unless strong and consistent project management standards are in place.

In addition to the PMBOK guidance covering individual projects, PMI also has guidance materials for program and portfolio management, discussed in a section following. Program management generally refers to a series of related projects, and portfolio management covers standards for a suite of projects and programs within an enterprise. PMI also has a professional project manager certification program, where members who complete a professional examination and satisfy experience requirements are certified as a PMP (Project Management Professional). The PMI and its PMBOK guide have become the de facto standards for many project management activities in the enterprise both in the United States and worldwide.

EXHIBIT 16.1 Definition of a Project Following PMBOK Guidance

A project is a temporary endeavor undertaken to create a unique product, service, or result. The temporary nature of projects indicates a definite beginning and end. The end is reached when the project's objectives have been achieved or when the project is terminated because its objectives will not or cannot be met, or when the need for the project no longer exists. Temporary does not necessarily mean short in duration. Temporary does not generally apply to the product, service, or result created by the project; most projects are undertaken to create a lasting outcome. For example, a project to build a national monument will create a result expected to last for centuries. Projects can also have social, economic, and environmental impacts that far outlast the projects themselves.

Every project creates a unique product, service, or result. Although repetitive elements may be present in some project deliverables, this repetition does not change the fundamental uniqueness of the project work. For example, office buildings are constructed with the same or similar materials or by the same team, but each location is unique—with a different design, different circumstances, different contractors, and so on.

An ongoing work effort is generally a repetitive process because it follows an organization's existing procedures. In contrast, because of the unique nature of projects, there may be uncertainties about the products, services, or results that the project creates. Project tasks can be new to a project team, which necessitates more dedicated planning than other routine work. In addition, projects are undertaken at all organizational levels. A project can involve a single person, a single organizational unit, or multiple organizational units.

A project can create:

- A product that can be either a component of another item or an end item in itself,
- A capability to perform a service (e.g., a business function that supports production or distribution), or
- A result such as an outcome or document (e.g., a research project that develops knowledge that can be used to determine whether a trend is present or a new process will benefit society).

The sections following provide a general introduction to PMBOK and its importance as a major standard for developing and managing projects. Our objective is not to provide a detailed description of these PMBOK standards but to introduce them as an important IT governance tool for managing enterprise projects. When an enterprise IT organization is using project management techniques to develop new applications or other systems processes, they should be developed using an accepted project management standard such as PMI's PMBOK or PRINCE2, another important standard also described in a section following.

PMBOK STANDARDS

A Web search for books on the subject of project management yields thousands of titles, covering all aspects and variations of project management. The better ones

today, however, are based on the PMI's PMBOK, an almost de facto standard describing all aspects of project management. Here we provide an overview of the PMBOK process, with an emphasis on how it can be useful for improving and enhancing project management activity IT governance functions.

PMBOK standards have been regularly updated, with each new set of guidance materials building on the previous versions. The PMBOK's version 4, released in 2008, defines the project management as five basic process groups and nine knowledge areas that are elements of almost all projects. Applicable to projects, programs, portfolios, and operations, these concepts have become a framework for effectively launching and executing IT-related and other projects. PMBOK's five basic project management process groups are:

1. **Initiating.** There should be formal processes in place to launch any project effort, including a description of the project's objectives, estimated budgeting, and appropriate approvals. This is an important IT governance requirement.
2. **Planning.** Every project requires planning in terms of time and resource estimates as well as for the linkages between components and other projects that require coordination. Project planning is particularly important because many projects are structured across organizational lines and staffed with multiple part-time resources building the project elements.
3. **Executing.** This PMBOK process group defines the actual project activities: what needs to be done to accomplish project goals. From an IT perspective, these activities may range from searching for appropriate software tools to customizing the software to meet user requirements and then implementing the project after the completion of appropriate internal controls testing and user education.
4. **Controlling.** An important component in overall governance of project activities, processes should be in place to monitor the completion of key project elements, determining that budgets and objectives are being met.
5. **Closing.** The final process requires wrapping up the project effort, then both delivering the project components and summarizing and reporting the project results. Going back to our original definition of a project, the effort should have a definite end where its results can be summarized and any next steps planned in a future but separate project effort.

PMBOK matches each of these five project management processes with nine project management knowledge areas in terms of their inputs and outputs as well as tools and techniques. Project inputs include the documents, plans, and necessary resources to launch the project with the planned outputs and, of course, the completed project materials. To go from the starting project inputs to the completed end product, a wide range of tools and mechanisms is necessary. A project to build a house, for example, would need lumber, a plan, and other supplies, including nails and roofing materials, as the inputs. A hammer and a saw as well as knowledge of carpentry also are tools necessary to get started on the construction. The output in this simplified example is the completed house.

Although much more complex than requiring just lumber, a hammer, and nails, the launch of many IT systems implementation projects requires a firm statement

of objectives, a detailed project plan, resource plans, testing plans, and many other detailed specifications. The IT team building the project needs to gain an understanding of the areas of concern; tools such as laptop systems to perform, build, or launch project components; and knowledgeable IT specialists to build, test, and implement the effort. In many respects, the construction of a single-residence frame house is a relatively small and simple project compared to many IT applications and infrastructure efforts. Most IT projects launched by enterprises of any type are complex, and this complexity is what has led to PMI and its PMBOK best practices standards. Prior to these standards, enterprises too often launched major project efforts without adequate preparation. The results were often massive cost and time overruns as well as failures even to complete the project. Many other non-IT projects had the same enterprise problems. All lacked consistent and thorough project management approaches.

PMBOK has defined the project management process as taking place in a consistent and well-controlled manner. In addition to the five basic project management process groups, the PMBOK guidance defines nine project management knowledge areas:

1. Project integration management
2. Project scope management
3. Project time management
4. Project cost management
5. Project quality management
6. Project human resources management
7. Project communications management
8. Project risk management
9. Project procurement management

The PMBOK guidance describes each of these knowledge areas in considerable detail in terms of their inputs, tools, and outputs. For example, PMBOK's Project Time Management knowledge area description includes input, tools, and output sections on:

- **Defining project activities.** This is the process of identifying specific actions to be performed to produce project deliverables.
- **Sequencing critical project activities.** The relationships between project activities should be identified and documented.
- **Estimating activity resources.** Estimates should be made for the types and quantities of people, materials, equipment, and supplies required to perform scheduled project activities.
- **Estimating activity durations.** There is a need to analyze the project activity sequences, durations, resource requirements, and time and resource needs to create project schedules.
- **Developing project schedules.** A plan review progress is necessary to monitor the status of projects to update their achievements and to manage any changes to their schedules.

These are basic steps to manage time for any project, and they certainly are the key activities an enterprise IT function should consider when planning the time requirements for any IT-related project.

In addition to guidance on general management, PMBOK details project management tools and processes needed in each of these knowledge areas. Exhibit 16.2 summarizes these PMBOK processes and knowledge areas. This chapter's objective is not to provide a detailed overview of all of PMBOK's processes and knowledge areas but to emphasize the role of PMBOK for planning and implementing effective IT project management processes. The reference numbers in Exhibit 16.2 are based on PMBOK materials, but the point here is that they emphasize the steps necessary to build effective projects. For example, knowledge area number 7 is project cost management, necessary steps for any project process. Exhibit 16.2 shows the necessary process groups, estimating the costs, building a budget, and controlling those costs.

ANOTHER PROJECT MANAGEMENT STANDARD: PRINCE2

PRINCE2 is another and increasingly recognized project management standard. It is a process-driven standard and more closely tied to the ITIL guidance materials discussed in Chapter 6. PRINCE2 was first released in 1996 as a generic project management method. While not yet that common in the United States, PRINCE2 has become increasingly popular and is now a de facto standard for project management in the United Kingdom and European Union countries. PRINCE2 is a process-driven project management standard based on a set of defined project management principles and processes. Exhibit 16.3 describes the PRINCE2 project management process.

Compared to PMBOK, the PRINCE2 standard is more prescriptive and business case–driven than PMBOK. It is also more oriented to project management and controls by senior management than the direct project management team. In many respects, it is a better IT governance tool for managing and controlling projects. However, a goal of this chapter is not to describe how to implement the PRINCE2 project management standard but only to highlight it as an alternative tool to PMBOK for managing and controlling IT projects.

A management team reviewing and helping to establish project management IT governance controls should insist that the IT organization follow established standards for planning and controlling its project activities. Many today may be using PMBOK, which is consistent with effective IT governance. However, if an IT function has not embraced PMBOK, management should consider recommending that the IT function adopt PRINCE2 standards, as they comply closely with the ITIL best practices discussed in Chapter 6.

IT SYSTEMS PORTFOLIO AND PROGRAM MANAGEMENT

Project managers often use the term *program* when discussing multiple projects. A program usually is a senior-level project used to manage a series of related or connected projects. For example, an enterprise may want to implement some fairly large initiative that is divided into a series of separate projects. Each of the projects can operate

EXHIBIT 16.2 PMBOK Process Groups and Knowledge Areas Summary

Knowledge Area		Project Management Process Groups				
		Initiating Process Group	**Planning Process Group**	**Executing Process Group**	**Monitoring & Controlling Process Group**	**Closing Process Group**
4	Project Integration Management	4.1 Develop Project Charter	4.2 Develop Project Management Plan	4.3 Direct & Manage Project Execution	4.4 Monitor & Control Project Work 4.5 Perform Integrated Change Control	4.6 Close Project or Phase
5	Project Scope Management		5.1 Collect Requirements 5.2 Define Scope 5.3 Create Work Breakdown Struct.		5.4 Verify Scope 5.5 Control Scope	
6	Project Time Management		6.1 Define Activities 6.2 Estimate Resources 6.3 Estimate Activity Resources 6.4 Estimate Durations 6.5 Develop Schedule		6.6 Control Schedule	
7	Project Cost Management		7.1 Estimate Costs 7.2 Determine Budget		7.3 Control Costs	
8	Project Quality Management		8.1 Plan Quality	8.2 Perform Quality Assurance	8.3 Perform Quality Control	
9	Project Human Resources Management		9.1 Develop Human Resources Plan	9.2 Acquire Project Team 9.3 Develop Project Team 9.4 Manage Project Team		
10	Project Communication Management		10.2 Plan Communications	10.3 Distribute Information 10.4 Manage Stakeholder Expectations	10.5 Report Performance	
11	Project Risk Management		11.1 Plan Risk Management 11.2 Identify Risks 11.3 Perform Quantitative Risk Analysis 11.4 Qualitative Risk Analysis		11.6 Monitor & Control Risks	
12	Project Procurement Management		12.1 Plan Procurements	12.2 Conduct Requirements	12.3 Administer Procurements	12.4 Close Procurements

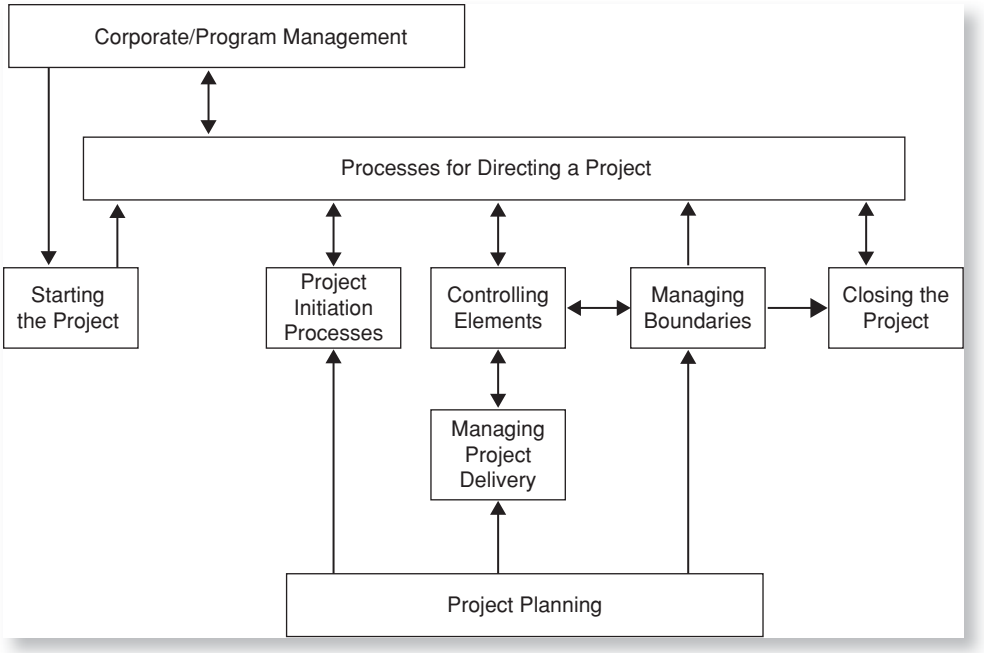

EXHIBIT 16.3 PRINCE2 Project Management Process

independently, but a program structure manages all of them together. This chapter generally uses the term *project* for one single effort and *program* for multiple but related projects. Another term, a *portfolio of IT investments*, usually refers to a suite or inventory of existing project investments. Multiple and related projects usually are grouped together into programs and project portfolios.

A *project management program* consists of a series of related projects managed in a coordinated way to obtain benefits and controls that would not be available if these projects were managed separately and individually. *Programs* generally consist of related work that may be outside the scope of the individual projects.

The need for program management generally occurs when an enterprise has some single objective that can best be achieved through a series of separate projects. For example, a plan to move a manufacturing facility to a new location would require a series of separate projects that all require coordination. One project here might require moving and setting up production equipment, another would move raw materials, and still another separate project would cover doing IT systems conversions. Although someone should be in charge of coordinating all of these efforts, each project has separate needs and requirements. They would be managed separately but grouped together as a program.

IT governance should think of the requirements for a series of related IT audit projects as a program. For example, the enterprise may be asked to review Sarbanes-Oxley (SOx) Section 404 internal controls within a series of facilities. Even though each of these separate projects would potentially take place at different types of facilities with different geographic locations and responsible IT management teams, each has similar high-level objectives, and a senior manager might be responsible for the overall

completion of each one. These groups of projects might be organized and managed as a program, with the individual IT project managers all reporting to a program manager for the overall compliance effort.

Moving up another level, *portfolio management* refers to collections of projects, programs, and other work that are grouped together to facilitate their effective management. If separate IT groups existed for two units in a corporation, with perhaps one covering IT infrastructure operations in European Union countries and the other for the United States and Canada, the overall IT activities for each could be considered as an IT function portfolio with both classified under a higher-level portfolio at the

EXHIBIT 16.4 Project, Program, and Portfolio Management Overview

	Project	**Programs**	**Portfolios**
Scope	Projects have defined objectives. Scope is progressively elaborated throughout the project life cycle.	Programs have a larger scope and provide more significant benefits.	Portfolios have a business scope that changes with the strategic goals of the enterprise.
Change	Project managers expect change and implement processes to keep change managed and controlled.	Program managers must expect change from both inside and outside the program and be prepared to manage it.	Portfolio managers continuously monitor changes in the broad environment.
Planning	Project managers require planning to evolve from high-level to detailed planning throughout the project life cycle.	Program managers develop the overall program plan and create high-level plans to guide detailed planning at the component level.	Portfolio managers create and maintain necessary processes and communications relative to the aggregate portfolio.
Management	Project managers manage the project team to meet the project objectives.	Program managers manage the program staff and the project managers; they provide vision and overall ownership.	Portfolio managers may manage or coordinate portfolio management staff.
Success	Success is measured by product and project quality, timeliness, budget compliance, and degree of customer satisfaction.	Success is measured by the degree to which the program satisfies the needs and benefits for which it was undertaken.	Success is measured in terms of aggregate performance of portfolio components.
Monitoring	Project managers monitor and control the work of producing the products, services, or results that the project was undertaken to produce.	Program managers monitor the progress of program components to ensure that overall goals, schedules, budget, and benefits of the program will be met.	Portfolio managers monitor aggregate performance and value indicators.

corporate headquarters. These project, program, and portfolio management concepts are described in Exhibit 16.4. The idea is that reporting relationships should be established when necessary to promote efficiency and achieve overall objectives.

As well as for reviewing and managing individual IT projects and portfolios, the guidance in Exhibit 16.4 is useful to IT management where multiple but similar IT audit projects can be managed as a program or considered as part of a project portfolio. The whole idea is that there should be a tight interaction between programs or portfolios and their individual or subordinate projects, but program management often does not totally drive or dictate individual project activity, and the separate projects will help to define the overall structure of the supporting programs. The analogy between a series of individual IT audits and the overall audit function is very strong.

Many IT functions today are burdened with multiple project and program initiatives—some well organized, but others that are not well connected and even seeming to be messy. As an important component of IT governance, there should be ongoing efforts to streamline the management of these strategic project-related initiatives. The IT governance solution is to build a strong foundation of project portfolio management. Effectively managing project requests, resources, budgets, and projects is key to delivering IT governance initiatives that drive the company forward and become a sure path to helping the enterprise reach its goals.

THE PROGRAM MANAGEMENT OFFICE (PMO), A STRONG GOVERNANCE RESOURCE

As discussed previously, a program is a senior-level project that serves as a vehicle to manage and supervise other, subordinate projects. This concept got started in IT, where for years IT departments struggled to deliver projects on time and within budget. A solution was to rein in projects more closely through the establishment of program management offices (PMOs) as a way to boost IT efficiency, cut costs, and improve on project delivery in terms of time and budget. What has worked for IT projects can work equally well for all projects in an enterprise.

The PMO may provide standards, an approval authority for all projects, or even project management skills from the staff of certified project management professionals. A PMO function can instill much-needed project management discipline in IT departments and all other groups involved with project management. PMOs can help by providing the structure needed to both standardize project management practices and facilitate project portfolio management, as well as determine methodologies for repeatable processes. The Sarbanes-Oxley Act—which requires companies to disclose investments, such as large projects, that may affect a company's operating performance—is also a driver, since it forces companies to keep a closer watch on project expenses and progress.

There are two basic models of PMOs: One acts in a consulting capacity, providing project managers in business units with training, guidance, and best practices; the other is a centralized version, with project managers on staff who are loaned out to business units to work on projects. How a PMO is organized and staffed depends on

myriad organizational factors, including targeted goals, traditional strengths, and cultural imperatives. When deployed in line with an IT organization's culture, a PMO can help the enterprise to deliver strategic projects that satisfy both the internal and external customers. Over time, a PMO should be able to provide savings to the enterprise by enabling better resource management, reducing project failures, and supporting those projects that offer the biggest payback.

PMOs are usually administrative functions supporting IT management and can vary in terms of their size, structure, and responsibilities. They provide project management guidance to project managers in business units and often function in the following support areas:

- **Project management process/methodology.** Whether the enterprise IT function uses PMBOK or PRINCE2, the PMO can provide guidance to develop and implement consistent and standardized project management processes.
- **Project management training.** This is often an effective area where the PMO can conduct project-related training programs or collect requirements for an outside company.
- **Home for project managers.** With the PMO as a central source for project management knowledge and support, it can maintain a centralized office from which project managers are loaned out when a designated project ends.
- **Internal consulting and mentoring.** With a goal to promote project management excellence, the PMO can advise other employees about best practices with an emphasis on PMBOK.
- **Project management software tools.** Project management tools can be selected and maintained for use by all project participants. Many software tools are available to support project management activities. A PMO can act as a clearinghouse on the use of these tools.
- **Portfolio management.** Establish a staff of program managers who can manage multiple related projects, such as infrastructure technologies, desktop applications, and so on, and allocate resources accordingly.

There may different approaches for an organization to manage a PMO function, but a centralized approach, typically marked by hands-on control over projects, often is most effective at organizations where the PMO regularly interacts with senior executives and has the power to cancel and prioritize projects. Using well-defined project management methodologies, the PMO often works with business units on every aspect of project management—from defining initial requirements to post-implementation audits. Maintaining consistent processes across the organization enables an organization to break down projects into manageable components and thereby minimize failures.

The responsibilities of PMOs range widely, from providing a clearinghouse of project management best practices to conducting formal portfolio management reviews. A PMO's oversight need not be limited to just project development and may include the coordination and tracking of both projects and services. Coming up with a PMO that works for any given organization is an exercise in both customization and patience. When it comes to establishing a PMO, there are limited roadmaps to follow, benchmarks

to shoot for, or metrics against which to measure. The most effective PMOs are those that reap improvements over time and continuously push the organization to improve on its performance.

PROJECT MANAGEMENT, THE PMO, AND IT GOVERNANCE

Enterprises build and install their IT and other major initiatives through the use of projects. As we have discussed, IT projects and project management frequently operate outside of regular organizational boundaries. An initiative to implement a new manufacturing costing system, for example, might involve resources from IT systems and programming as well as people from the accounting and various manufacturing functions. Under a designated project manager, the effort can find resources and take the necessary steps to implement the manufacturing costing system.

The effective use of project management principles is an important component of effective IT governance. The IT organization should have embraced a project management standard, such as PMBOK. More important, there should be evidence that all active projects are using that standard and that they have active project planning mechanisms in place as well as such documentation as firmly stated project objectives and quality assurance plans in place. There should be evidence of orderly processes in place to manage IT projects.

If IT management is using project processes to build and manage many of its activities, and if there are large numbers of related projects, the IT organization should establish an effective set of PMO processes. Program management is an important process whenever a large number of project processes are used to build and implement IT projects and processes. Effective IT project management processes will improve overall IT governance processes.

NOTE

1. Project Management Institute, *A Guide to the Project Management Book of Knowledge (PMBOK Guide)*, 4th ed. (Newtown Square, PA: 2008).

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER SEVENTEEN

Service Level Agreements, itSMF, Val IT, and Maximizing IT Investments

MANY YEARS AGO, THE VERY FIRST MAINFRAME COMPUTER SYSTEMS were installed in major corporations with objectives of streaming operations and cost savings and sometimes also for a bit of corporate prestige. These were the early days when those very expensive mainframe systems were often located in glass-walled enclosures in corporate lobbies with high expectations of the savings the business would gain from this then-new technology. Disappointment soon followed, however. Because of safety and space concerns, those mainframe computers, with their growing array of tape drives and mass storage units, were soon moved to remote corporate locations. Even more important, the investment savings were usually not very rapid due to the cost of recruiting and building an IT specialist staff, the time delays and costs associated with many IT development projects, and application software that did not work as well as expected. Enterprises soon realized there was a need to review and attempt to gain an increased benefit from their IT investments at all levels.

This chapter reviews IT governance issues and concerns from multiple perspectives regarding an enterprise's investment in IT resources. We will first discuss the importance of effectively installing and managing IT service level agreements (SLAs) as part of an enterprise's IT operations. SLAs and related service management guidance are one of the ITIL best practices that were first introduced in Chapter 6. They are understandings or internal contracts between the users of IT services and the IT department. They describe the services that IT will provide to user departments, including updated files and reports as well as the timely delivery of specified files and documents. We will emphasize the importance of SLAs as an IT governance tool and discuss how to more effectively implement and gain benefits from enterprise SLAs.

Closely related but separate from ITIL, the IT Service Management Forum (itSMF) is a separate professional membership organization that has promoted IT service

management processes and has published some related guidance in these areas. With local chapters in many major cities and with a strong interest in IT governance issues, the itSMF is an organization that a management professional may be interested in further exploring. This chapter will introduce this professional group and highlight some of its IT governance strengths.

The chapter will also briefly introduce the Open Compliance and Ethics Group (OCEG) and its GRC standards.

The chapter will provide some additional detail on this group's governance standards, with an emphasis on its "Red Book." We will almost certainly see increased emphasis on these OCEG standards as tools to improve IT governance in future years. This chapter will discuss some of the standards and tools that the itSMF has released to improve IT governance, business risk, and fraud.

The Information Systems Audit and Control Association (ISACA), introduced in earlier chapters, has developed and released a set of guidance materials, called *Val IT*, for better understanding and evaluating the investments that an enterprise devotes to its IT resources. This chapter will introduce the Val IT model and describe why it can be an important concept for helping general management and its IT functions to better work together in achieving greater value from their IT processes.

The chapter will conclude with some general guidance for an enterprise on measuring and achieving value from its IT investments. We have gotten a lot smarter over the years, as our massive and expensive mainframe systems have largely gone away and we now frequently assemble new applications from a menu of options that reside in a cloud-based system rather than building them with an in-house development staff. Nevertheless, enterprises need to recognize the cost of these systems and take actions to achieve maximum value. This is an important element of IT governance.

ITIL SERVICE MANAGEMENT BEST PRACTICES AND THE ITSMF

Chapter 6 introduced ITIL and its best practices standards for IT service support and service delivery. Providing effective guidance and support for the enterprise IT function and many areas of IT governance, ITIL processes cover areas more closely aligned with the smooth and efficient operation of the overall IT infrastructure. Although highlighted with the other best practice processes in Chapter 6, an understanding and implementation of ITIL's service level management best practices is particularly important for today.

Service level management is the name given to the process of planning, coordinating, drafting, agreeing, monitoring, and reporting on formal agreements between both the enterprise IT function and the providers and recipients of IT services. These processes are formalized through service level agreements (SLAs) between IT and the customers or users of IT applications, processes, and other services. SLAs represent a formal agreement between the providers of services to IT and the IT end-user customers. When the first ITIL service level best practices materials were published in 1989, an SLA was an interesting but not very common concept. Today, many enterprises have introduced them—although with varying degrees of success—and senior managers should be

familiar with and understand the importance of SLAs when understanding internal IT infrastructure controls.

As an example of an SLA, when an enterprise IT function contracts for an outside provider, such as for disaster recovery backups, the arrangement should be covered by a formal contract where the disaster recovery provider agrees to provide certain levels of service, following some time-response-based schedule. The governing contract here would be called an SLA between IT and the provider of continuity services. SLA agreements between IT and its customers are even more important here, from an internal control perspective. We have used the term *customer* for the older and still common term of *IT users*. There are many groups in an enterprise that use the terminology *IT's services*, and as its customers, they have expectations of certain levels of service and responsiveness. These arrangements are defined through an SLA, a documented agreement between IT and its customers defining the key service targets and responsibilities of both parties. The emphasis should be on agreement, and SLAs should not be used as a way of holding one side or the other to ransom. Also, we are not talking about the need for a formal, legal type of document but just a documented understanding between the parties. A true partnership should be developed between the IT provider and the customer for a mutually beneficial agreement; otherwise, the SLA could quickly fall into disrepute and a culture of blame may prevent any true service quality improvements from taking place.

In an SLA, IT promises to deliver specified services per an agreed-on set of schedules and understands that there will be penalties if these service standards are not met. The goal is to maintain and improve on service quality through a constant cycle of agreeing, monitoring, reporting, and improving the current levels of IT service. SLAs should be strategically focused on the business and maintaining the alignment between the business and IT.

Exhibit 17.1 outlines the contents of a typical SLA. This should not be the type of document that would look like a home mortgage signed as part of a house closing. Rather, the IT customers would use it to document the IT service requirements that they are seeking, such as "average response times no more than . . ." or "financial systems close processing completed by . . ." or other factors. To temper expectations and show what could be available, an IT function usually provides a service offerings catalog. Customer IT services requirements should be negotiated and formal SLAs established. Performance against these SLAs should be monitored on an ongoing basis with performance reported regularly. Failure to meet these SLA standards could result in additional negotiations and SLA adjustments. This SLA process provides benefits for the business and IT, including:

- Because IT should be working to meet negotiated standards, IT services will tend to be of a higher quality, causing fewer interruptions. The productivity of the IT customers should improve as well.
- IT staff resources will tend to be used more efficiently when IT provides services that better meet the expectations of its customers.
- By using SLAs, the services provided can be measured and the perception of IT operations will generally improve.

EXHIBIT 17.1 Sample IT Service Level Agreement Contents

While there is no one form or format for an IT service level agreement, the following elements should be considered as contents for most SLAs:

Agreement introduction pages

- Parties to this agreement.
- Title and brief description of the agreement.
- Dates: start, end, and review.
- Scope of the agreement; what is covered and what is excluded.
- Responsibilities of both the **Service provider** and the **Customer**.
- Description of the **Services** covered.

Service hours

- Hours that each service is normally required (e.g., 24x7, Monday to Friday 08:00–18:00).
- Arrangements for requesting service extensions, including required notice periods (e.g., request must be made to the **Service Desk** by 12 noon for an evening extension, by 12 noon on Thursday for a weekend extension).
- Special hours allowances (e.g., public holidays).
- Service calendar.

Availability

- Availability targets within agreed hours, normally expressed as percentages. The measurement period and method should be stipulated and may be expressed for the overall service, underpinning services, critical components, or all three. Since it is difficult to relate to simplistic percentages, Availability can be measured in terms of the Customer's inability to carry out its business activities.

Reliability

- Usually expressed as the number of service breaks, or the Mean Time Between Failures **(MTBF)** or Mean Time Between **System** Incidents **(MTBSI)**.

Support

- Support hours (where these are not the same as Service hours), including arrangements for requesting support extensions.
- Required notice periods (e.g., request must be made to the Service Desk by 12 noon for an evening extension, by 12 noon on Thursday for a weekend extension).
- Special hours allowances (e.g., public holidays).
- Target time to respond to Incidents, either physically or by other method (e.g., telephone contact, e-mail).
- Target time to resolve Incidents, within each **Incident Priority**—target varies depending upon Incident priorities.

Throughput

- Indication of likely traffic volumes and throughput activity (e.g., the number of transactions to be processed, number of concurrent Users, amount of data to be transmitted over the network).

Transaction response times

- Target times for average, or maximum workstation response times (sometimes expressed as a percentile—e.g., 95% within 2 seconds).

Batch turnaround times

- Times for delivery of input and the time and place for delivery of output.

(*Continued*)

EXHIBIT 17.1 (*Continued*)

Changes

- Targets for approving, handling, and implementing RFCs, usually based upon the **Category** or **Urgency**/priority of the Change.

IT service continuity and security

- Brief mention of IT Service Continuity Plans and how to invoke them, and coverage of any security issues, particularly any responsibilities of the Customer (e.g., backup of free-standing PCs, password Changes).
- Details of any diminished or amended service targets should a disaster situation occur (if no separate **SLA** exists for such a situation).

Charging

- Details of the charging formula and periods (if charges are being made). If the **SLA** covers an **Outsourcing** relationship, charges should be detailed in an Annex as they are often covered by commercial in confidence provisions.

Service reporting and reviewing

- The content, frequency, and distribution of service reports, and the frequency of service review meetings.

Performance incentives/penalties

- Details of any agreement regarding financial incentives or penalties based upon performance against service levels. These are more likely to be included if the services are being provided by a third-party organization. It should be noted that penalty clauses can create their own difficulties.

- Services provided by third parties are more manageable with the underpinning contracts in place, and any possibility of negative influence on the IT service provided is reduced.
- Monitoring overall IT services under SLAs makes it possible to identify weak spots that can be improved.

The SLA process is an important component of IT operations. If an enterprise does not use formal SLAs, senior management should consider recommending implementing formal SLA processes. SLAs can create a totally new environment within IT, where all parties will better understand their responsibilities and service obligations, with the SLA as a basis for resolving many issues.

Professionals seeking to broaden their understanding of IT service management should use the resources of itSMF, discussed previously. This not-for-profit organization is a prominent player in the ongoing development and promotion of IT service management best practice standards. The business executive interested in learning more can access www.itsmfi.org for additional information. A search will lead to the sites of independent, country-by-country national sites. This is a membership organization, but one can obtain a guest registration and gain access to many white paper documents and information about upcoming conferences and seminars. The itSMF is very concerned with promoting ITIL service management best practices and has a strong interest in the ISO 20000.

OPEN COMPLIANCE AND ETHICS GROUP (OCEG) STANDARDS

The Open Compliance and Ethics Group (OCEG) is an industry-led nonprofit organization that develops standards and helps enterprises enhance their governance, risk management, and compliance processes. With major support from the technical industry, it has published several "standards" such as a GRC capability model. We have placed the word "standards" in quotation marks because the OCEG does not have the standards-setting authority as might be found in the AICPA's standards or even in some of the ISO guidance materials discussed in Chapter 7.

This section introduces the OCEG's "Red Book," its GRC capability model. These OCEG guidance materials are very similar to other GRC and IT governance framework guidance information found in other chapters, but with a slightly different emphasis or approach. As part of its name, OCEG's use of "Open" has some special meaning in an IT sense. An open system regularly exchanges feedback with its external environment to continuously analyze that feedback, adjust internal systems as needed to achieve the system's goals, and then transmit necessary information back out to that environment. Closed systems, unlike open systems, have hard boundaries through which little information is exchanged. Organizations such as bureaucracies, monopolies, and stagnating IT systems that have closed boundaries often can appear to be unhealthy. A common term in many newer, advanced IT systems today, *open* is an appropriate word for this GRC capability model.

The OCEG's GRC guidance is found in a document named Capability Model "Red Book" and is located at www.oceg.org. The basic document, at version 2.0 at the time of publication, is available through the Internet, while an enhanced version is available to subscribing members. The basic Internet edition contains a complete description of this GRC model, but at an additional cost, the enhanced version with templates and other help aids is useful to implement this tool. The capability model is based around a concept called Principled Performance, an integrated GRC approach that we will discuss in the sections following.

The GRC capability elements view, shown in Exhibit 17.2, represents the heart of the OCEG model. Many of the concepts are very similar to GRC concepts discussed in other chapters, but the OCEG model has a more industry- and IT-focused view. OCEG's objectives of this model should help enable an enterprise to:

- Enhance business objectives
- Enhance organization culture
- Increase stakeholder confidence
- Prepare and protect the enterprise
- Prevent, detect, and reduce adversity
- Motivate and inspire desired conduct
- Improve responsibility and efficiency
- Optimize economic and social value

OCEG's Principled Performance Concept

OCEG has trademarked the term *Principled Performance* to describe the need for an articulation of an enterprise's financial and nonfinancial objectives to achieve all of the

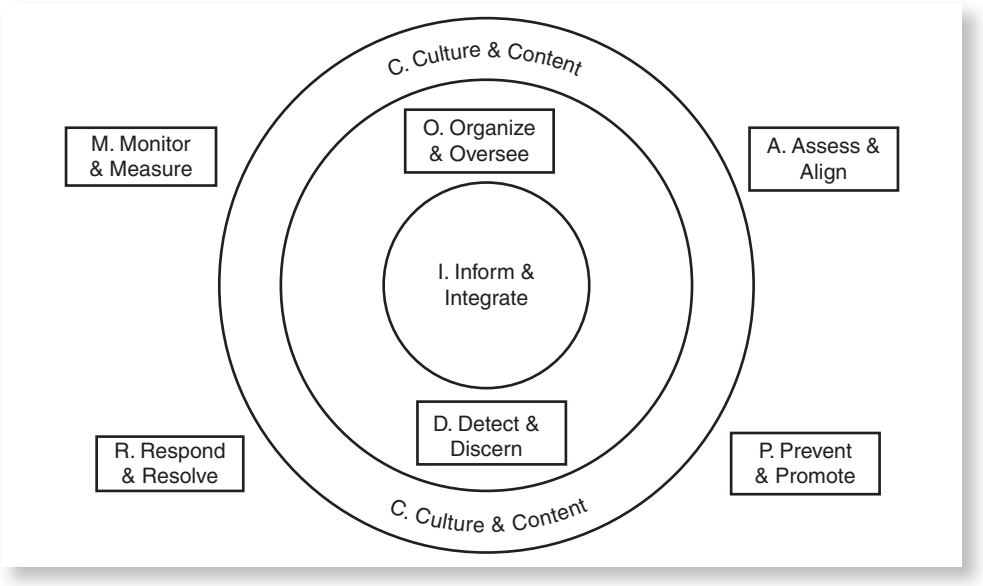
C. Culture & Content
O. Organize & Oversee
M. Monitor & Measure
A. Assess & Align
I. Inform & Integrate
D. Detect & Discern
R. Respond & Resolve
P. Prevent & Promote
C. Culture & Content

EXHIBIT 17.2 OCEG GRC Capability Model Elements

objectives it chooses to pursue while employing an effective, efficient, and responsive approach to supporting governance, risk management, and compliance objectives. The concept here is that all enterprises must operate within defined external and internal boundaries where outside forces, such as legal and regulatory requirements, establish the mandated external boundaries. The objective is to integrate GRC principles and objectives to help an enterprise more effectively drive performance.

For an enterprise to achieve OCEG's concept of Principled Performance, it must clearly define its mission, vision, and values and define the objectives it seeks to achieve. It must define how it will pursue these objectives while also addressing risks and uncertainty, protecting and creating value, identifying new opportunities, and staying within defined boundaries of ethical conduct. The enterprise should make these choices transparent to appropriate internal and external stakeholders and attempt to accomplish all of this using an integrated approach to achieve the highest possible level of performance.

These Principled Performance concepts are key elements of the OCEG's GRC capability model as shown in Exhibit 17.2, paraphrased from the OCEG materials. The following sections describe the elements of that model in greater detail. This model outlines at a very high level an extensive set of materials and concepts that are part of the OCEG model. The interested reader is encouraged to access the full model through the previously referenced Web address.

GRC Capability, Context, and Culture Elements

Exhibit 17.2 shows capability, context, and culture as factors or elements in an enterprise GRC model. The objective of this exhibit is to illustrate the external and internal business contexts and current culture in which an enterprise operates, such that the

GRC system can address current realities and identify opportunities to adapt the context and culture to define the enterprise's values to better achieve desired outcomes. Using the letter *C*, there are four elements to this section of the published GRC model:

C1 External Business Context
C2 Internal Business Context
C3 Culture
C4 Values and Objectives

The GRC capability model further defines a set of subelements for each of these. For example, for C3, the model contains the following subelements:

C3.1 Analyze Ethical Culture
C3.2 Analyze Ethical Leadership
C3.3 Analyze Risk Culture
C3.4 Analyze Board Involvement
C3.5 Analyze Governance Culture and Management Style
C3.6 Analyze Workforce Engagement

Each of these is supported by more detailed elements to expand the outline. In addition, the model contains a set of principles and a list of common sources of failure for each as well as guidelines and references for additional support materials.

GRC Capability, Organize, and Oversee Elements

The objective of the OCEG guidance is to organize and describe a GRC system that it is integrated with and, when appropriate, that modifies existing business processes. This set of elements, marked with the letter *O*, in the OCEG model consists of the following elements and subelements:

O1 Outcomes and Commitment
  O1.1 Define GRC System Scope
  O1.2 Define GRC System Styles and Goals
  O1.3 Obtain Commitment to the GRC System
O2 Roles and Responsibilities
  O2.1 Define and Enable GRC System Oversight Rules and Accountability
  O2.2 Define and Enable Management Roles and Responsibilities
  O2.3 Define and Enable Leadership Roles and Responsibilities
  O2.4 Define and Enable GRC System Operational Rules
  O2.5 Define and Enable Assurance Roles and Accountability (e.g., internal audit)

With an outline of detailed sub and sub-subpoints, there is sufficient detail here to help an enterprise establish and organize a GRC function. There are good sets of principles and common sources of failure for each to help organize an effective GRC process for an enterprise.

An objective of this chapter is to highlight that the OCEG GRC capability model contains some excellent materials to help an enterprise establish an effective GRC function and improved IT governance processes. We are merely highlighting some of the high-level attributes of this model, and each of these elements is supported by more detail.

Our objective is not to go around the OCEG model and comment on each element. Rather, we are highlighting here that the OCEG model provides some excellent guidance for considering some important elements for establishing important IT governance processes.

Other OCEG Elements

Moving around Exhibit 17.2, each section of the model contains specific section objectives. For example, the stated goal of the guidance behind GRC model's A section, labeled Assess and Align, is to optimize the organization risk profile with a portfolio of risks, tactics, and activities. The actions here include risk identification, analysis, and optimization. For example, the objective for Risk Identification in the published model is to "Identify events, forces, and factors that may affect the achievement of business objectives, including those arising with noncompliance with the requirements established by law, standards, internal policies or other . . . boundaries."

Moving around the capability model, the P, or Prevent and Promote, section's objective is to promote and motivate desirable conduct and prevent undesirable events and activities, using a mix of controls and incentives. This section has seven elements, including Codes of Conduct, Preventive Controls, and Stakeholder Relations and Requirements.

Highlighting another GRC capability model element, R, or Respond and Resolve, has an objective to respond to and recover from noncompliance and unethical events or GRC system failures, so that the organization resolves each immediate issue and prevents or resolves similar issues more effectively and efficiently in the future. This element has five components:

R1 Internal Review and Investigation
R2 Third-Party Inquiries and Investigations
R3 Corrective Controls
R4 Crisis Response, Continuity and Recovery
R5 Remediate the GRC System

Many of these procedures go beyond the IT governance steps described in other chapters to investigate violations in enterprise ethics and compliance practices. For example, for R1 on internal reviews, the guidance is to review and be prepared to investigate allegations or indications of misconduct or GRC system failures to understand the facts, circumstances, root causes, and appropriate resolution. The principle here is that the board and senior management should never be blindsided but instead must know in a timely fashion about any issue that can significantly affect the enterprise.

The standard calls for an enterprise to establish procedures and a core team for inquiring further into and investigating complaints or reports about compliance or

ethical issues, as well as issues detected during ongoing monitoring or periodic evaluation of the GRC system. The standard goes on to call for strong procedures to bring certain matters to the attention of senior management or the board. Another guidance standard calls for an enterprise to periodically review any reported incidents and data to identify trends, trouble spots, or controls in need of revision. The suggested procedures are stronger than we would expect to find in many enterprises today.

Moving further around the six GRC elements here, the Monitor and Measure component is located in the upper-left side of the diagram. This element contains guidance to assign management specific responsibility, decision-making authority, and the accountability to achieve system goals. Using the letter *M,* it consists of the elements to monitor and evaluate the performance of the GRC programs and to initiate systems improvements where necessary.

This element recognizes that the GRC system must be flexible enough to respond rapidly to internal and external changes in the environment in which it operates. It will be most effective if an enterprise identifies and evaluates anticipated changes in time to plan system alterations. The model recognizes that the failure to respond to any needed context changes may result in the failure of IT governance standards and critical GRC system controls.

The standard calls for an enterprise to continually monitor internal and external changes that may have a direct, indirect, or cumulative effect on the enterprise. For example, the changes in external requirements may include:

- Laws, rules, and regulations
- Administrative guidelines and rulings
- Significant judicial rulings
- Regulatory and prosecutorial guidance
- Consent orders and enforcement activities
- Standard and trade association commitments

This list points out the challenge an enterprise—particularly a large, multinational organization—will face when attempting to monitor such events as governmental rulings. It is often too much to assign such monitoring to one group because of the breadth and diversity of information. Processes should be in place that encourage managers at all levels and locations to report potential warning areas to a central GRC administrative group for further investigation and planned actions.

The I, or Inform and Integrate, component is the last element in the GRC model. In Exhibit17.2, it is located in the center of the model with an overall objective to capture, document, and manage GRC information so that it efficiently flows up, down, and across the extended enterprise and to and from external stakeholders. This calls for the enterprise to develop and implement a wide range of GRC information processes to classify, capture, store, and report processes. While it is not necessary for an enterprise to have one system throughout, they all should be consistent in terms of their taxonomies, formats, and communications abilities.

The construction of a set of GRC supporting systems can be a key factor in the success of total GRC information but may be one of the key challenges to achieving success.

Similar to other COSO ERM concepts discussed in Chapter 8, an enterprise must capture and classify a wide variety of disparate data and information and also must have the ability to capture those materials for analysis and to respond to inquiries.

The OCEG Model and IT Governance

We have not yet reached the point where an interested manager can Google a request for "OCEG GRC compliance control systems" and receive a list of appropriate offering vendors in return. There are many approaches for solutions but few obvious single solutions. A possible area of solutions can be found in hospital electronic medical record systems (EMRS), where every activity of a patient, from laboratory test results, to doctor's notes, to prescribed medications and more, is captured for later retrieval on the EMRS for current use and for archival purposes. An effective GRC capability model information system should have many of these elements.

The preceding sections have outlined many elements of the OCEG GRC capability model on a very high level. Other models call for a more detailed and sometimes more administrative controls-oriented approach. Our high-level description here, however, does not give justice to the full study that can be found in the OCEG's 240-page publication in its basic form, with much more detail in the extended document. The interested reader is encouraged to further investigate the OCEG GRC model.

A visit to the OCEG Web site will allow open access to a variety of materials, with some for review and others for subscribers. Of particular interest may be its Red Book, an assessment document to support OCEG's capability model guidance. Its purpose is to provide GRC professionals with a common set of assessment procedures that align with the previously outlined GRC capability model as well as guidance on what can be expected during an assessment of any GRC system, with goals to help an enterprise evaluate the design and operating effectiveness of its GRC system as well as to reduce the cost of such evaluations by providing specific procedures. A further goal of this publication is to raise the overall level of maturity and quality of an enterprise's GRC processes by helping to create prioritized improvement plans and to provide an external source for the judgment and recognition of these practices.

Level and Scope of the OCEG Standards-Setting Authority

As we have emphasized, the OCEG at present does not have the standards-setting authority as found in the PCAOB or the ISO. In addition, although it has released some strong guidance materials, that information still does not have a high-level of recognition at this time. Nevertheless, we feel that the importance of the OCEG and its guidance materials will only grow in future years as concerns and need for effective GRC processes grow.

A major strength of the OCEG is that it is totally a volunteer organization managed by staff members from sponsoring organizations and formed into an OCEG leadership council. Sponsors include the major public accounting firms such as Pricewaterhouse-Coopers and Grant Thornton. In addition, there are many major IT industry leadership sponsors such as Oracle and SAP as well as primarily U.S. industry sponsors from such firms as Aon, the major insurance company, and the retailer Walmart. If there is any

concern here, it appears that based on its sponsoring organizations and committee members, the OCEG is more of a U.S-based, and not truly international, organization. In our global world today, we need more of an international focus.

VAL IT: ENHANCING THE VALUE OF IT INVESTMENTS

All enterprises, large or small, exist to deliver value to their stakeholders. These enterprises face a critical challenge in ensuring that they realize value from their increasingly large-scale and complex investments in IT resources. The IT Governance Institute (ITGI), first introduced in Chapter 5, has released a set of best practices materials called *Val IT*[1] to help enterprises address this challenge and realize value from these IT-related investments.

Val IT attempts to address IT management and governance problems faced by management at all levels. IT technologies and practices are always changing and adapting to new business practices. Enterprises frequently invest in new and revised systems and procedures with little additional planning or study, soon to find that their new initiative does not work as well as promised or requires a much larger investment than anticipated. We frequently encounter this situation when, for example, an enterprise chief financial officer is frustrated by some shortcoming in the enterprise's financial systems, personally sees a potential better solution at a vendor-sponsored trade show, and then encourages the IT function to adopt that solution. With such pressure from a member of senior management but little detailed investigation beyond that, enterprises sometimes embark on new IT investments at significant cost and without really getting much value from those investments. Val IT is a best practices governance framework that is closely aligned with the Control Objectives for Information and related Technology (COBIT) framework (discussed in Chapter 5). COBIT consists of a set of guiding principles and a number of recommended IT-related processes that conform to those principles and key management practices. Val IT encompasses a comprehensive set of research activities, publications, and auxiliary services supporting the core Val IT framework, as illustrated in Exhibit 17.3. Although COBIT sets good practices for the *means* of contributing to the process of value creation, Val IT defines good practices for the *ends*, by providing enterprises with the structure they require to measure, monitor, and optimize the realization of business value from their investments in IT.

Many enterprises today, regardless of their size, revenue, industry, region, or business activity, make large-scale investments in IT systems and related information technology resources. However, in far too many cases, this IT value simply is not realized. For example, a 2007 survey by the IT research firm Gartner found that 20 percent of all expenditures on IT are wasted[2]—a finding that represents, on a global basis, an annual destruction of value totaling about $600 billion. Similarly, a 2009 survey of Fortune 1000 chief information officers by Goldman Sachs found that, on average, 40 percent of all IT spending brought no return to the enterprise.[3] The point here is that many enterprises do not measure the value of or assess their ongoing IT investments. This is a significant loss from an IT governance perspective.

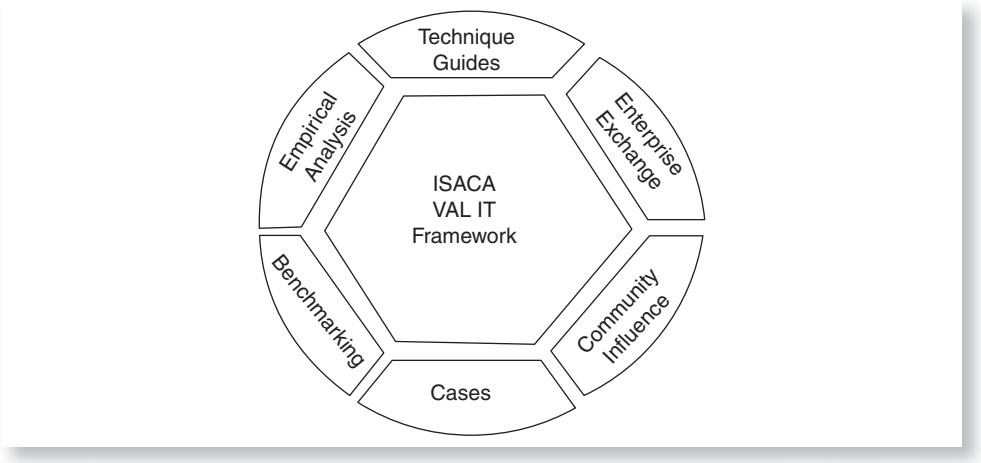

EXHIBIT 17.3 Val IT Framework

The ITGI's Val IT materials[4] provide guidance for assessing the value of IT investments. Creating IT-enabled values, however, is not easy. Most enterprises commonly exhibit one or more of the following symptoms, which have been summarized adapted from the published Val IT guidance materials:

- **Problems in delivering technical capabilities.** Many enterprises have IT functions that are not mature enough to effectively and efficiently deliver the technology capabilities needed to both support business operations and enable business change. This challenge highlights the need to improve IT governance and management processes either before or in conjunction with the introduction of value management practices.
- **Limited or no understanding of IT expenditures.** Senior enterprise managers frequently do not have a sufficiently transparent view of their IT expenditures and IT-enabled investments across all IT services, assets, and other resources. Often decision makers can only estimate how much they are investing in IT, what benefits they are gaining for the expense, and what the full business rationale for the commitment might be. Expenditures frequently are sourced from many different uncoordinated budgets, resulting in significant duplication and conflict in demand for resources. In addition and all too often, management does not focus on IT costs and pricing issues in its IT application budgeting reviews.
- **Business abdication of decision making to the IT function.** When the roles, responsibilities, and accountabilities of an enterprise's IT function are unclear, IT functions tend to usurp the driver's seat, determining which IT-enabled business investments should be pursued, prioritizing these based on the IT function's limited insights, and inappropriately relieving the business of its responsibility in defining and defending the business rationale used to justify every single IT-enabled investment decision.

- **Communication gaps between the IT function and the business.** Close collaboration between IT operations and other business functions is crucial to IT value creation. When such a partnership is absent, communication suffers, inefficiencies mount, synergies fail to emerge, and the work environment tends to devolve into a culture of blame. In some cases, the IT function is too often relegated to the role of a follower instead of innovator, and is engaged in investment proposals too late in the decision-making process to contribute significant value. In other cases, the IT function is blamed for not delivering value from IT-enabled investments—value that only other business functions, in partnership with the IT function, can deliver.
- **Questioning the value of IT.** Ironically, even though enterprises continue to invest more and more in technology resources, many key executives often question whether appropriate value is actually realized from these investments. Frequently, the dominant focus is on managing IT costs rather than understanding, managing, and leveraging IT's role in the process of creating concrete business value. As IT-enabled investments increasingly involve significant organizational change, the failure to shift focus from cost to value continues to be a major constraint to realizing value from these IT-related investments.
- **Major investment failures.** When IT projects stumble, the associated business costs can be enormous—and highly visible. Project cancellations can trigger unexpected and very expensive impacts across the business, and related budget overruns can starve other projects of crucial resources. All too often, these problems are ignored until it is far too late to take any corrective action.

These symptoms can be found in many enterprise IT functions. All too often, IT has led its business partners with requests for new priorities and services without looking at their overall value to the enterprise as a whole. The Val IT materials should encourage all parties to take a harder look at the value being received from IT investments and services. Perhaps even more important, Val IT gives senior managers an opportunity to focus on areas for realizing greater value from IT operations governance processes.

Launching an IT Value Management Initiative

The ITGI Val IT materials are designed to provide guidance to enterprise IT functions, the senior management funding IT resources, and all stakeholders benefiting from those IT activities. However, because this best practices guidance is published from an ISACA-related source (and not, for example, in a corporate board member type of publication), this material may not get sufficient necessary attention at senior management. However, Val IT is an excellent set of materials for supporting IT governance and to support internal controls improvements.

Senior management should discuss IT value management issues with both IT and operations management and consider launching an IT value management initiative. One of the best ways to assess the enterprise's readiness to undertake a value management program is to review and evaluate the Val IT framework's principles and the extent of its commitment to implement them. These principles include:

- IT-enabled investments should be managed as a portfolio of investments, as discussed in Chapter 14.
- IT-enabled investments should include the full scope of activities required to achieve their business value.
- IT-enabled investments should be managed through their full economic life cycle.
- Value delivery practices throughout the enterprise should recognize that there are different categories of investments, which will be evaluated and managed differently.
- Value delivery practices should define and monitor key metrics and respond quickly to any changes or deviations.
- Value delivery practices should engage all stakeholders for appropriate accountability and the delivery of capabilities and realization of business benefits, with ongoing monitoring, evaluations, and process improvements.

IT managers and senior managers involved in IT processes for an enterprise are—or should be—the ones directly involved in overseeing or carrying out value management practices. Based on the Val IT materials, an enterprise IT and business managers should meet to assess their readiness to move to IT value management. Exhibit 17.4 provides questions and readiness checks for IT management to assess an enterprise's readiness to move to IT value management.

IT management should consider the questions and points outlined in Exhibit 17.4 in terms of whether the enterprise and the operations management team is aware of the importance of value management and has taken steps to implement this concept. Of course, all parties—IT and operations management—need to be sold on the importance of IT value management.

EXHIBIT 17.4 IT Value Management Readiness Assessment

1. Are all IT-enabled investments, such as applications, networks, and server connections, managed as a portfolio of investments?
2. Are all IT-enabled investments managed to include the full scope of activities required to achieve their business objectives for the investment?
3. Are IT-enabled investments managed through their full economic life cycle, from the costs of launching or purchasing the investment through regular operating costs and then to retirement?
4. Do IT and management recognize there should be different categories of value delivery investments that should be evaluated and managed differently?
5. Have value delivery key metrics been defined to monitor and respond quickly to any changes or deviations?
6. Do the established value delivery practices appear to engage stakeholders and assign appropriate accountability for the delivery of capabilities and the realization of business benefits?
7. Is there a continuous monitoring and improvement process in place over all value delivery practices?

The value management published guidance calls for an enterprise to become more involved with value management best practices. It calls for enterprises and stakeholders with initial insight into value management to develop an understanding and awareness of, and commitment to, value management principles and practices. Based on this initial assessment, a more detailed maturity analysis can be initiated based on the Val IT domains of IT value governance, portfolio management, and investment management.

Getting Started in Value Management

Val IT concepts are important for effective IT governance. An effective way to start a value management process is to assess current readiness using the readiness assessment questions of Exhibit 17.4. Once the assessment has been completed, the results will provide the basis for identifying what is needed to evolve from the current to a future value management state and for establishing the priorities for what needs to be improved.

Based on ITGI's published Val IT materials, the following five steps outline how to implement Val IT and value management in an enterprise. Differences between enterprises can be vast, and the Val IT guidance materials describe only a limited number of starting points:

Step 1: Build awareness and understanding of value management. In many enterprises, key decision makers and stakeholders do not adequately appreciate the need to create value. This concept of value does not just naturally emerge from normal business plans or activities; it has to be actively created. The problem is that while the concepts of value management have been around for decades, the notion of value creation and preservation through business change in modern enterprises is usually treated as an implied principle, not a conscious and pervasive tenet to guide behavior.

For many enterprises, there is no shared understanding of what constitutes enterprise value, what level of effort is required to realize it, or how to measure value. As a result that impacts many enterprises, opportunities to realize value may be missed or fail in execution, and the concept of value is often eroded or destroyed.

Enterprise operational, financial, and IT managers need to establish a broad-based awareness of the need for value management and to nurture an understanding of what is required to develop this capability, including a strong internal executive and management commitment to improving and sustaining value creation over time.

With a strong understanding of value management, organizational and individual behaviors should change to take a broader enterprise-wide view and a more disciplined, value-driven approach to decision making. This should result in an increased understanding and acceptance of the need for IT and the other business functions to work together in partnership, supported by clear roles, responsibilities, and accountabilities related to value management, leading to more value realization from IT-enabled investments.

Step 2: Implement improved IT governance. Processes, roles, responsibilities, and accountabilities related to realizing value from IT-enabled investments need to be

clearly defined and accepted. All too often, the roles, responsibilities, and accountabilities of IT are unclear when contrasted with other business functions. Business decisions sometimes are made by the IT function while IT decisions are made by the business. In this environment, a culture of blame can predominate, with persisting confusion regarding accountability, responsibility, and sponsorship.

An enterprise needs to establish an IT governance framework with clearly defined roles, responsibilities, and accountabilities. This framework should be supported by strong and committed leadership, appropriate processes, organizational structures and information, and a well-aligned reward system. Under such an IT governance framework, organizational and individual attitudes and behaviors should evolve toward a broader, more strategic enterprise perspective. Executives and managers from IT and operations should take a more disciplined, value-driven approach to their decision making and accountability. With improved IT governance, an environment of more and efficient decision making should lead to increased trust between the IT function and the rest of the business. The result should be an increased realization of value from IT-enabled investments.

Step 3: Undertake an inventory of IT investments. For most enterprises, little, if any, visibility exists into the number, scope, and cost of current and planned IT-enabled investments or the resources either allocated or needed to support these investments. All too often, overall IT expenditures across the enterprise are not known, and often they come from many different and uncoordinated budgets, with significant duplication. In many enterprises, extensive conflict in the demand for IT resources exists.

As a solution, an enterprise should establish portfolios of proposed and active IT investments, IT services, assets, and other resources. This concept is even greater than the ITIL configuration management best practices discussed in Chapter 6. As a result of establishing these portfolios, organizational and individual attitudes and behaviors should change to take a broader enterprise view. The appropriate processes and practices must be in place to support this.

The benefits from such an inventory of IT investments are an increased understanding of exactly what is being spent on which IT investments, in which areas of the business, and by whom. Another benefit is better identification of opportunities to increase value through improved allocation of funds, reductions in overall enterprise cost by eliminating redundancies, more effective use of resources, and reduction in risk from a better understanding of these IT portfolios.

Step 4: Clarify the value of individual IT investments. For many if not most enterprises, there is no consistently applied process for determining the value of potential or current IT investments. That value could be defined as the total life cycle benefits net of total life cycle costs adjusted for risk, based on the time value of money. As a result, some stakeholders persistently question whether IT investments have generated value. Business cases for IT-enabled investments are often nonexistent or poorly prepared and usually are considered by IT management as merely an administrative checklist required to secure funding. Little, if any, preinvestment information exists on IT costs, nor is there any analytical rigor in defining these benefits or value. Few metrics exist to enable the monitoring of what, if any, value

is to be or has been created. All too often, it is assumed that technology, or the IT function, will magically deliver value.

An enterprise should establish a process to develop and update comprehensive and consistently prepared business cases for its IT-enabled investments, including all of the activities required to create value. The business case should be developed through a top-down approach, starting with a clear articulation of the desired business outcomes and progressing to a description of what actions need to be accomplished and by whom. These business cases should be updated and used as an operational tool throughout the complete economic life cycle of the IT investment.

As a result of this process, organizational and individual attitudes and behaviors should change to put more effort into the planning of IT investments and the development and regular updating of business cases. A more objective assessment of IT investment business cases enables better and more objective comparisons across different types of IT investments. There are better opportunities to compare individual investments based on their relative value against other investments available and a stronger track record for selecting the best. There should also be less uncertainty and risk that the value projected will not be realized.

Step 5: Conduct IT investment evaluations, prioritizations, and selections. Currently there is no consistently applied process for objectively evaluating the relative value of all proposed and current IT-enabled investments—especially with respect to prioritizing and selecting those IT investments with the highest potential value. Today, many enterprise IT investment decisions are subjective and often highly political. Once a decision is made to proceed with an investment, it is rarely revisited unless some crisis occurs. Poorly performing IT investments are rarely remediated or canceled early enough to mitigate losses; if they are canceled, they are regarded as failures for which someone should be held accountable.

The Val IT solution is to implement portfolio management disciplines to categorize IT-enabled business investments. An enterprise should establish and rigorously apply criteria to support consistent and comparable evaluations of the investments throughout their full economic life cycle. As a result, organizational and individual attitudes and behaviors should change to take a broader enterprise view and embrace greater transparency.

The benefit of this five-step approach should be an increased opportunity to create value through selecting IT investments with the greatest potential to deliver value. This opportunity should be followed by active management of those investments and early cancellation of them when it is apparent that value cannot be realized. The Val IT materials provide more detail on these approaches.

Val IT provides useful guidance and proven processes and practices for the governance, selection, and management of IT-enabled investments. Val IT describes the interrelated processes that need to be in place if enterprises are to secure optimal value from their investments. This section has merely highlighted and extracted some of the materials from the Val IT guidance materials. Val IT is an IT governance concept that is very useful for assessing IT relative values in both the launches of new IT applications and management's building of general controls. More important, these Val IT concepts

should be communicated to IT and senior management so they can better understand their investments in IT resources.

NOTES

1. Val IT Framework for Business Technology Management, www.isaca.org/KnowledgeCenter/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx?utm_source=multiple&utm_medium=multiple&utm_content=friendly&utm_campaign=va.
2. IT Financial Management, Gartner Consulting, www.gartner.com/it/products/consulting/GTACaseStudy.pdf.
3. Independent Insight: IT Spending Survey, "2009 Under the Knife—Expect –1% Global Decline," Goldman Sachs, November 2, 2009, www.scribd.com/doc/7737986/Goldman-Sachs-IT-Spending-Survey.
4. John Thorp, "Val IT Framework 2.0—Adding Breadth and Depth to the Value Management Road Map," *ISACA Journal* (June 2008): 1–3.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

PART FIVE

Monitoring and Measuring Enterprise Management and Board Governance

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER EIGHTEEN

Enterprise Content Management

AN IT MANAGEMENT TERM that was not that common before the early years of this century, *enterprise content management (ECM)* describes the strategies, methods, and tools used to capture, manage, store, preserve, and deliver the content and documents related to organizational processes. Now a fast-growing set of IT activities, ECM is the series of processes covering the management of information within the entire scope of an enterprise no matter whether that information is in the form of a paper document, an electronic file, a database print stream, e-mail documents, data stored in an IT cloud, or any of the many other evolving forms of data and information. ECM processes are primarily aimed at managing the life cycle of information from initial publication or creation all the way through archiving and eventual disposal.

ECM aims to make the management of corporate information and its supporting documents easier through simplifying storage, security, version control, process routing, and retention. The benefits to an enterprise using effective ECM processes include improved efficiencies, better controls, and reduced costs. For example, most banks today now have converted to using ECM processes to store paper copies of old checks versus the older method of keeping physical checks in massive paper warehouses. Under older, traditional systems, a customer request for a copy of a check might take weeks, as the bank employees had to contact a repository warehouse to have someone locate the right box, file, and check, pull the check, make a copy, and then mail it to the bank, which would eventually mail it to the customer. With an ECM system in place, the bank employee simply searches the system for the customer's account and the number of the requested check. When the image of the check appears onscreen, the employee is able to immediately e-mail it to the customer—usually while the customer is still on the phone.

Whether it is checks at a bank or any of a variety of other paper documents, effective ECM processes can reduce costs and improve operations. Effective ECM processes are important tools to help strengthen enterprise IT governance. This chapter introduces

ECM concepts and discusses areas where the business executive can improve overall IT governance processes through the implementation of ECM processes.

ECM CHARACTERISTICS AND KEY COMPONENTS IN THE ENTERPRISE TODAY

The factors that encourage businesses to adopt ECM solutions include overall needs to increase business transaction efficiency, improve the control of information, and reduce the overall cost of information management for the enterprise. ECM applications streamline access to records through keyword and full-text searches, allowing employees to get to the information they need directly from their desktops in seconds rather than searching multiple applications or digging through paper records.

ECM systems can enhance record control to help businesses improve customer service processes and comply with government and industry regulations such as Sarbanes-Oxley requirements, discussed in Chapter 2, or the Payment Card Industry Data Security Standard, included in Chapter 11. Security functions including user-level, function-level, and even record-specific security options also are important ECM components to protect sensitive data.

ECM can reduce storage, paper, and mailing needs, make employees more efficient, and result in better, more informed decisions across the enterprise—all of which reduce the overhead costs of managing information. ECM is particularly important when an enterprise has requirements for long-term document retention and requirements for high-volume capture. With our needs for specialized documents, ECM can help with signature-driven processes, rich media digital asset management, or technical/large-format drawing management, among others.

Enterprise content management, however, is not a closed-system solution or a distinct product category. ECM processes in an enterprise exist as just one catchall term for a range of established technologies and vendors in an enterprise. ECM is working properly when it is effectively "invisible" to users. ECM technologies support specialized applications as subordinate services and often are a collection of infrastructure components that fit into a multilayer model and include all document-related technologies in an enterprise for handling, delivering, and managing structured data and unstructured information jointly. As such, ECM processes are one of the necessary basic components of the overarching e-business application area.

ECM PROCESSES AND IT GOVERNANCE

ECM is an ongoing and evolving strategy for maximizing how all of an enterprise's information is to be used. ECM tools and strategies allow an enterprise to manage both its structured and unstructured business data and information wherever that information exists. Of course, it's not enough to just "manage" this information content. The ability to access the correct version of a document or record is important, but this content should be managed so that it is used to achieve business goals. The tools and

technologies of ECM can be important here to manage the complete life cycle of document content from birth to death.

ECM is an ongoing and evolving strategy for maximizing how an enterprise's information content should be used and can be fundamental to the success of enterprise business operations. While there are numerous software and other vendor offerings, management should think of implementing and using ECM in terms of the concepts of compliance, collaboration, continuity, and cost.

Despite the fact that enterprises today are facing massive increases in the numbers and complexity of their business and systems, many are still using the same document-by-document traditional methods of the past. An enterprise could realize some efficiencies and IT governance processes would improve through the adoption of enterprise ECM processes. As a starting point, management should review its document content life cycle. This concept is similar to our discussion on systems development life cycles (SDLCs) in Chapter 15. Here, a management and IT team should map current document and information flow processes to see where they may find overlaps and room for improvement in business applications and information flow strategies.

The information gathered will typically show the complexities inherent in processes that deal with managing an organization's content. The objective should be to build enterprise ECM architecture, as shown in Exhibit 18.1, which may include many if not all of the following elements:

- **ECM document capture.** ECM processes should be focused on the storage, tracking, and use of all documents, whether paper, digital, or rich media documents such as video, logos, or photographs. Document repositories should handle structured and unstructured documents, recognizing that digital assets typically have high intellectual property value. A document repository can be a sophisticated system that costs hundreds of thousands of dollars, or as simple as a file folder system in a smaller company. The key is to have information that can be found once it is placed in the system.
- **User experience and collaboration tools.** Collaboration is the art of working together, and is key here to ECM-related technologies such as instant messaging, whiteboards, online meetings, and e-mail facilities that allow work to take place wherever and whenever needed. Collaboration allows individuals with complementary or overlapping areas of expertise to create better results faster than before, allowing business units and teams to work together anytime—whether in adjoining offices or a world apart.
- **Workflow life cycles.** Tools are necessary to move content throughout identified business process cycles, such as claims processing. ECM tools should be used to develop, deploy, monitor, and optimize multiple types of automation applications, including processes that involve both systems and people. Workflow life cycles are also associated with the manual processes of managing documents, and they should handle approvals and prioritize the order documents are presented. In the case of exceptions, workflow also escalates decisions based on predefined rules developed by system owners.

- **ECM records management.** While any piece of content can be designated a record, these items should be managed following a retention schedule that determines how long a record is kept based on either outside regulations or internal business practices. There are needs to store these multiple and diverse records such that they can be retrieved when needed and eventually deleted at appropriate future times.
- **Web content tools, including rich media.** ECM processes should address the content creation, review, approval, and publishing processes of their Web-based content. Key Web content data includes creation and authoring tools or integrations, input and presentation template design and management, content reuse management, and dynamic publishing capabilities.
- **ECM collaboration and social computing tools.** Collaboration technologies enable individual users, such as employees or business partners, to easily create and maintain project teams, regardless of geographic location. These technologies and social computing tools facilitate collaborative, team-based content creation and decision making for both traditional IT systems and the growing number of social network computing processes in the enterprise. There is a need to maintain appropriate records of these activities.
- **Research and content analytics.** Whether because of marketing strategies, governmental mandates, or other factors, enterprises have increasing needs to review and analyze many of their business transactions. While we have strong database tools to help, ECM processes can very much help to retain the results of these activities.
- **Continuity and retention tools.** Keeping a business going 24/7 is the task of continuity planning, and because the lifeblood of most enterprises today is represented by electronic documents, ECM has a key role to play in continuity management. ECM technologies allow for the creation of centralized repositories where all vital corporate information can reside. The method of storage will vary depending on how critical the content is to the company—from off-site backup tapes to redundant, mirrored sites separated by geography and on different power grids. An enterprise must prioritize its content to determine how quickly the document content needs to be back online in the event of a disaster, and mission-critical processes and the entities on which they are dependent must be determined, followed by a business impact assessment to determine the impact of a disruption or the loss of those processes. Strong ECM processes are a key here.
- **ECM customer engagement facilities.** Tools to allow an enterprise, its customers, and other stakeholders to easily retrieve and access all levels of transaction activities should be a major feature of ECM processes. These are the types of tools that allow a customer service facility to quickly supply purchase histories, rather than having to go back and retrieve records.
- **Document management.** ECM processes here help organizations to better manage the creation, revision, approval, and consumption of electronic documents. Document management provides key features such as library services, document profiling, searching, check-in, checkout, version control, revision history, and document security.
- **Enterprise interoperability links.** An enterprise today typically has the need to share data and information between its various operating units and outside stakeholders. Although different systems and formats can cause difficulties,

ECM processes should be open and flexible enough to build systems interoperability links covering the overall enterprise and its operating units.

- **ECM security tools.** ECM processes should restrict access to content, both during its creation and management when delivered. These security processes should include:
  - **Digital rights management.** ECM processes should prevent the illegal distribution of rights-managed content by restricting access to content down to the sentence level as well as granting/restricting permissions for forwarding and accessing content.
  - **Digital signatures**. Processes should ensure the identity of a document sender, and the authenticity of messages.

Two other elements of the Exhibit 18.1 EMC architecture framework should not be ignored. The top box or section on this chart is an area called *compliance management*. The key to a successful ECM compliance strategy is the need to integrate their idea of ECM compliance into the business and not view compliance as a project that can be completed and then considered "finished." While painful, complying with regulations should be viewed as an opportunity to improve common business processes and not just an ongoing cost to the business. This level of compliance is a bit different than the GRC compliance component of IT governance.

Developing a compliance initiative properly will tap many areas of enterprise expertise, particularly legal, IT, and records management, all in support of the overall business objectives of the enterprise. Individuals from each of these areas should contribute their knowledge and perspectives to ensure the benefits of a sound compliance program. While compliance is not always a technology problem, information technology, and the massive growth of unstructured content, contributes to corporate exposure. The tools of ECM, properly used, can help reduce the overall cost of compliance to the business and improve overall IT governance, shown as the lower element of Exhibit 18.1.

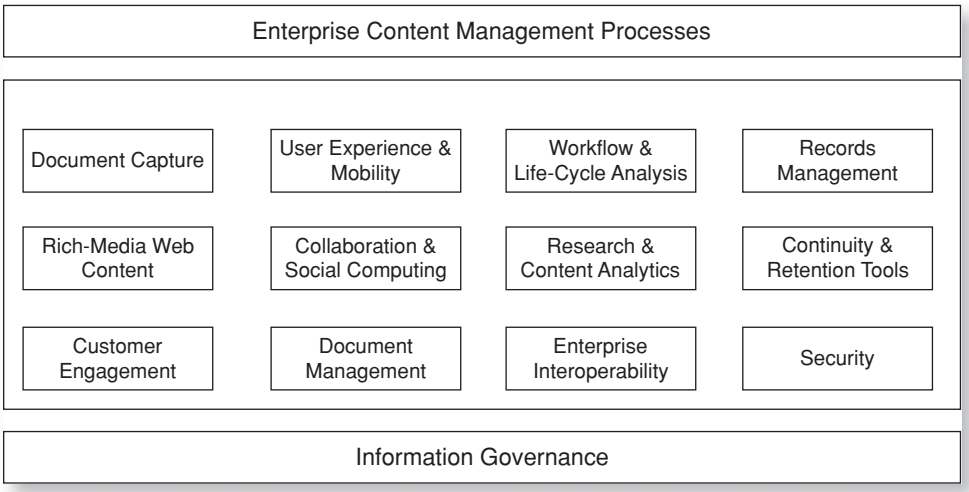

EXHIBIT 18.1 ECM Architecture

CREATING AN EFFECTIVE ECM ENVIRONMENT IN THE ENTERPRISE

As mentioned in the introductory comments to this chapter, ECM is not just a single system but is more of an enterprise strategy and is typically a series of systems and processes to better manage the multiple forms and formats that an enterprise deals with today, ranging from paper documents to Twitter notes, engineering drawings, and much more. Some enterprise IT functions have developed an ECM strategy and may have largely implemented that ECM strategy approach. Others may have implemented some effective ECM components, such as an order verification customer service system, but still have a ways to go before launching overall ECM. Then there may be some enterprises that just have not addressed the concept and are continuing to use their traditional document-by-document approaches.

Effective ECM processes can be a very good way to improve enterprise IT governance. Exhibit 18.2 outlines some of the requirements that management should consider when adopting an ECM strategy. If an enterprise is facing one or more of these requirements, particularly several of them in a significant manner, it may benefit from a move to ECM.

The move to ECM requires some form of strategy as a first step. Some of the options for developing a strategy for an enterprise-wide move to ECM include:

- Build a new, first-time, on-premises, enterprise-wide ECM platform using offerings from a single vendor's ECM suite.
- Migrate and replace all existing content management systems to the new enterprise-wide, single-vendor ECM product.
- Migrate all existing content management systems to the selected existing, enterprise-wide, single-vendor ECM product.

EXHIBIT 18.2 Enterprise Requirements Justifying a Move to ECM

- Long-term records retention or requirements.
- Logistical needs for physical records management and retrieval.
- High-volume information or records capture needs.
- Needs to comply with record management standards (e.g., federal government or ISO).
- Case management project environment.
- Significant signature-driven record or document processes.
- Digital asset management (rich media).
- Technical/large-format drawing management.
- Facilities or asset management requirements.
- Outward/customer-facing Web portals.
- Needs for outside the firewall partner inclusions.
- Heavy-duty process management applications.
- Print/output/transmittal management needs.
- Tight integration with ERP/CRM/LOB systems.
- Multichannel inbound systems communications.
- Digital rights/high-value asset management requirements.
- High-security data encryption requirements.

- Selectively update/replace/migrate existing multiple departmental/local systems as needed.
- Install new dedicated/specialist departmental systems as required to achieve local objectives.
- Move to a cloud-based ECM suite provided by a third party.

The objective of this chapter is not to outline the details of implementing an enterprise-wide ECM strategy using elements that have been established or to work with a major software vendor such as IBM or EMC that can supply the guidance and tools. The following sections describe the key elements of an overall enterprise ECM system or set of processes. An effective ECM should contain elements of most of these.

Enterprise ECM Features: Archiving

Businesses today are forced to deal with a dizzying array of disparate corporate and departmental data sources, including relational databases, document repositories, e-mail stores, and file servers. Compounding the challenge of managing this complex data source environment are requirements surrounding corporate acquisitions, regulatory legislation, information governance, and mandates to reduce operational cost through vendor and infrastructure consolidation. An enterprise needs to establish ECM document archive repositories to store these often millions of statements, policies, images, and other customer-facing documents. The archive should capture individual documents for discovery, content validation, storage organization, retrieval, distribution, and delivery.

ECM archive indexes are typically associated with document content at the point of creation by composition engines, or during uploading into an archive. Design is important here, since once documents are in an archive, it is very difficult to enhance or augment these indexes to meet changing business needs or needs for differing customer views.

While it can be a "nightmare project," ECM archiving offers an opportunity to clean up such matters as account number and naming standards that may be unique within a single organization but duplicated across acquired corporation records. In addition to launching a suite of ECM processes, archiving can bring both current and longer-range benefits to an enterprise.

Enterprise ECM Features: Classification Processes

ECM document classification processes automate the organization of unstructured content by analyzing full text of documents and e-mails. With content classification, IT can accelerate the time-to-value from enterprise content management investments such as content archiving or electronic records management. Classification processes should allow:

- The delivery of higher process investment returns by unburdening end users from manual tasks without risking inconsistent participation—while accurately categorizing large quantities of content.

- Filtering from document archives the e-mails and documents with limited business value.
- Organizing document content with consistent, reliable, and auditable logic.
- More readily adapting to changes in policies and categories by incorporating user feedback in real time.
- Establishing high-accuracy document classifications by combining multiple methods of classification such as:
  - Keyword rules and proximity matching.
  - Pattern extraction.
  - Highly accurate "learn by example" context-based approaches.

Content analytics is a key element to ECM document classification processes: It is an advanced search and analytics process to enable better decision making from enterprise content regardless of the source or format. Content analytics solutions can understand the meaning and context of human language and rapidly process information to improve knowledge-driven search and surface new insights from your enterprise content.

A more advanced process, content analytics typically uses more advanced natural language processing technologies such as the IBM Watson DeepQA, an advanced question-answering machine. A large amount of the information created and used by an enterprise is unstructured content and usually is growing at twice the rate of structured data. Harnessing that unstructured and semistructured information can help an organization work smarter, serve customers better, control costs, and plan for the future.

Enterprise ECM Features: Document Disposal and Governance Management

Document disposal and governance management should be an integral part of ECM processes. This process helps an enterprise to meet its obligations for information, manage information based on value, and dispose of information that lacks value or obligations at the earliest opportunity. The controlled disposal of information at the end of its utility can dramatically reduce information volume, operational complexity, and IT costs. With appropriate disposal and governance management solutions, IT can manage information based on its business value or legal obligations and dispose of the rest.

A key element of document disposal processes is that enterprise management and IT should gain document visibility into both legal obligations—such as legal holds and retention schedules—and the business value for specific information tied to the asset or an employee ID. ECM processes should have objectives for the real-time communication of requirements and facts between IT, records, and the enterprise legal staff through automatic action item assignments, notifications, alerts, and easy lookup of legal obligations.

An enterprise should practice defensible document disposal through accurate data inventories to eliminate excess stored data. By enabling IT to identify multiple copies of the same data, legacy data without business value or legal obligation, and duplicate systems, ECM processes can enable a company to retain only data with a potential

value. Appropriate ECM processes can prevent future unnecessary data buildup. When an enterprise practices defensible disposal, it can eliminate the risk of IT "saving everything," thereby increasing discoverable mass. In addition, it will help the enterprise from engaging in excessive or inappropriate disposal practices due to inconsistent processes and retention periods.

Office document management can be extended into hundreds of other solutions such as imaging, engineering applications, Web content management, XML-based content, and document publishing applications. Document management enables search and access to documents in these systems across the organization, while embracing industry-specific standards that help integrate with business processes. Document management extends the ECM infrastructure to include business documents created individually or via collaborative processes.

There are numerous vendor-supplied ECM technologies and solutions available today, but more important ECM is an ongoing and evolving strategy for maximizing how content is to be used. ECM information processes can be a starting point for an enterprise to review and establish a common information content life cycle. As a starting IT governance point, an enterprise should map its current systems and processes to identify overlaps and areas of room for improvement for the applications and strategies that it is developing. The information gathered may only hint at the complexity inherent in any process that deals with managing an organization's content. The next step should be to match up the technology tools to address the business's needs. Technology can enable streamlined management of content, but the underlying strategy must come first.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER NINETEEN

Internal Audit's Governance Role

THE PROFESSION OF AUDITING has been with us for a long time. Archaeologists have found that around 3000 BC the scribes in Mesopotamia utilized elaborate clay tablet accounting records that contained ticks, dots, and checkmarks indicating the existence of an auditing function. Auditing certainly has evolved over the millennia and today we generally classify most business auditors as either external or internal auditors. An external auditor is chartered by a regulatory authority to visit an enterprise or entity and to review and independently report the results of that review. In the United States, external auditors are generally certified public accountants, who are state-licensed and follow the standards of the American Institute of Certified Public Accountants (www.aicpa.org). There also are other types of external auditors in fields such as reviewing compliance for medical equipment devices, television viewer ratings, or in multiple governmental areas.

Internal auditing is a broader and often more interesting field. As an employee or member of an enterprise, an internal auditor independently reviews and assesses operations in a wide variety of areas, such as accounting office internal control procedures or manufacturing quality processes. Most internal auditors follow high-level standards established by their professional organization, the Institute of Internal Auditors (IIA; www.theiia.org), but there are many other different practices and approaches to internal auditing today due to its worldwide nature and the many types of auditing activities.

Some internal auditors specialize in reviewing enterprise financial internal controls, while others concentrate on business processes or operational issues. While all internal auditors today should have some knowledge of IT-related internal controls, there is also a strong professional specialty known as IT auditors. These professionals were introduced in Chapter 5 and are key resources for developing and implementing strong and effective IT governance processes.

This chapter reviews the importance of internal audit and IT audit in establishing effective IT governance processes. We will briefly review internal audit professional standards and activities that are important for establishing good IT governance practices. While internal audit is a separate and independent enterprise function, reporting only to an enterprise's audit committee board of directors, business executives should understand their roles and work with them to improve IT governance processes.

INTERNAL AUDITING HISTORY AND BACKGROUND

The senior business executive can better understand internal auditing and its key knowledge areas through some knowledge of internal auditors' professional organization, the IIA, and its published professional standards. This professional association defines the practice thus:

> Internal auditing is an independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization.

This definition is more meaningful when we focus on its key terms. *Auditing* suggests a variety of ideas that can be viewed very narrowly, such as the checking of arithmetical accuracy or physical existence of accounting records, or more broadly as reviews and appraisals at multiple organizational levels. Throughout this chapter, the term *auditing* will be used to include this total range of levels of service, from detailed checking to higher-level appraisals. The term *internal* means that the work is carried on within an enterprise, by its own employees, in contrast to external auditors, whose work is performed by outside public accountants or other parties, such as government regulators, who are not directly a part of the particular enterprise.

The remainder of this IIA definition of internal auditing covers other important terms that apply to the profession:

- *Independent* is used to indicate that internal auditing is free of restrictions that could significantly limit the scope and effectiveness of any internal auditor review or the later reporting of resultant findings and conclusions.
- *Appraisal* confirms the need for an evaluation that is the thrust of internal auditors as they develop their conclusions.
- *Established* confirms that internal audit is a formal, definitive function in the modern enterprise.
- *Examine* and *evaluate* describe the active roles of internal auditors, first for fact-finding inquiries and then for judgmental evaluations.
- *Its activities* confirm the broad jurisdictional scope of internal audit work that applies to all of the activities of the modern enterprise.
- *Service* reveals that the help and assistance to the audit committee, management, and other members of the enterprise are the end products of all internal auditing work.
- *To the organization* confirms that internal audit's total service scope pertains to the entire enterprise, including all personnel, the board of directors and their audit committee, stockholders, and other stakeholders.

Internal auditing should also be recognized as an organizational control within an enterprise that functions by measuring and evaluating the effectiveness of other controls. Internal auditors who do their job effectively become experts in what makes for the best possible design and implementation of all types of controls and preferred practices. This expertise includes understanding the interrelationships of various controls and their best possible integration in the total system of internal control. It is thus through the internal control door that internal auditors come to examine and evaluate all organization activities and provide maximum service to the enterprise. Internal auditors cannot be expected to equal—let alone exceed—the technical and operational expertise pertaining to the many various activities of an enterprise. However, internal auditors can help these responsible individuals achieve more effective results by appraising existing controls and providing a basis for helping to improve those controls as well as related IT governance practices.

Some background on the role of internal auditing might be of interest. Despite its ancient roots, internal auditing was not recognized as important by many enterprises and their external auditors until the 1930s. This recognition was primarily due to the establishment of the U.S. Securities and Exchange Commission (SEC) in 1934 and changing external audit objectives and techniques at that time. The United States as well as the rest of the world had then just gone through a major economic depression, by all accounts far more severe than the major worldwide recession that started in 2008. As a legislative corrective action, the SEC required that registered enterprises must provide financial statements certified by independent auditors. This requirement also prompted corporations to establish internal auditing departments, but with the primary objective of assisting their independent auditors. At that time, external financial auditors placed their emphasis on expressing an opinion on the fairness of an enterprise's financial statements rather than on detecting internal control weaknesses. The SEC rules precipitated auditing based on a limited sample of transactions, along with greater reliance on internal control procedures.

Internal auditors at that time were primarily concerned with checking accounting records and the detection of financial errors and irregularities; they were often little more than assistants to their independent external auditors, tasked with carrying out routine accounting reconciliations or serving as clerical support personnel. Vestiges of this old definition of internal auditing continued in some places even into the early 1970s. For example, in many retail organizations even up to the 1970s, the "auditors" were the people who counted cash and balanced cash registers (remember those?) at the close of the business day.

Although there were other voices that said something should be done to improve and better utilize the potential of internal auditors, things really got started after Victor Z. Brink completed his college thesis on internal auditing just before going off to serve in World War II. After the war ended, Brink returned to organize and head internal auditing for Ford Motor, and his college thesis was published as the first edition of what is now the standard reference book on the topic, *Modern Internal Auditing.*[1]

The IIA was launched at around the same time, in 1941, with its first membership chapter in New York, and Chicago soon to follow. The organization was formed by people who had been given the title of internal auditor by their enterprises and who wanted to

both share experiences and gain knowledge with others in this new professional field. A profession was born that has risen in stature and importance ever since.

The modern internal auditing of the 1940s required a very different professional skill set than today. For example, aside from some electromechanical devices and activities in research laboratories, digital computer systems did not exist. Enterprises had no need for computer programmers until early tabulating machines started to become useful for recordkeeping and other computational and accounting functions. Similarly, enterprises had very rudimentary telephone connections where switchboard operators routed all incoming calls to a limited number of desktop telephones. Today, of course, we have IT resources and are all connected through a vast, automated worldwide web of telecommunications, wireless connections, and the Internet. The increasing complexity of modern business and other enterprises has created the need for internal auditors to become ever-greater specialists in various business controls.

Those early internal auditors often played a very narrow role in their enterprises, with relatively limited responsibility in the total managerial spectrum. An early internal auditor often was viewed as a financially oriented checker of records and more of a police officer than a coworker. In some enterprises, internal auditors had major responsibilities for reconciling canceled payroll checks with bank statements or checking the mathematics in regular business documents.

Over time, the operations of many business enterprises increased in volume and complexity, creating managerial problems and new pressures on senior management. In response, many senior managers recognized the possibilities for better utilization of their internal auditors. Here were individuals already set up in an enterprise internal audit function, and there seemed to be every good reason for getting greater value from these individuals with relatively little increase in cost.

At the same time, internal auditors perceived these opportunities and initiated new types of services themselves. Thus internal auditors gradually took on broader and more management-oriented responsibilities in their work efforts. Because internal auditing was initially largely accounting-oriented, this upward trend was felt first in the accounting and financial-control areas. Rather than just reporting the same accounting-related exceptions—such as some documentation lacking a supervisor's initials—internal auditors began to question the overall control processes they were reviewing. Subsequently, internal audit valuation work began to be extended to include many nonfinancial areas in the enterprise.

New business rules and initiatives in the United States, such as the COSO (Committee of Sponsoring Organizations) internal control framework discussed in Chapter 4 or the Sarbanes-Oxley Act (SOx) requirements highlighted in Chapter 2, have caused a continuing increase in the need for the services of internal auditors. In addition, some newer environmental forces have created needs in such areas as protection from industrial hazards, support of quality-control programs, and different levels of business responsibility, including ethical standards. This need for ethical standards includes higher standards for corporate governance, greater involvement of boards of directors and their audit committees, a more active role for stockholders, and greater independence of the outside public accountant.

Today, internal audit has expanded its activities to all operational areas of the enterprise and has established itself as a valued and respected part of the senior management

effort. Today's internal auditor is formally and actively serving the board of director's audit committee, and the chief audit executive (CAE) today has a direct and active level of communication with that same audit committee. This overall situation reflects major progress in the scope of internal audit's coverage and level of service to all areas of the enterprise. The internal auditing profession itself, through its own self-development and dedication, has contributed to this progress and has set the stage for a continuing upward trend. It is an important component of effective IT governance processes.

INTERNAL AUDITING AND THE IT AUDITOR

We have discussed how the profession of internal auditing has evolved as well as the IIA, the worldwide internal audit professional organization. While any professional organization should assess the needs of its members in light of changing conditions, sometimes those changes can be a bit slow. This happened to the IIA with the explosive growth of IT systems and processes, starting perhaps in the early 1970s. A growing number of internal auditors at that time were realizing that these then-new IT systems and processes presented a wide range of new internal control issues, but their internal audit professional organization was not providing sufficient guidance or professional support.

A new professional organization, then called the EDP Auditors Association, was formed to support these new internal audit professionals. *EDP* stands for *electronic data processing,* an archaic term for IT systems and processes. These professionals are now known today as IT auditors and their key professional organization is now known as the Information Systems Audit and Control Association, an important IT governance professional organization that was first introduced in Chapter 5. IT auditors are often specialists in conventional internal audit departments, but are frequently associated with the major public accounting firms or operate as special consultants as well. They have a very important role in establishing and monitoring effective enterprise IT governance processes.

Senior business managers should understand the IT governance roles and responsibilities of the internal auditors in their enterprises, with particular attention given to their IT audit specialists. With its role of reporting to the audit committee of the board of directors, internal audit has a very special role and function in the enterprise. It generally operates as a collaborative type of function, setting its own schedule and activities but supporting senior management through reviews, activities, and assessments. The sections following discuss some of internal audit's important responsibilities in enterprise IT governance.

INTERNAL AUDIT'S IT GOVERNANCE ACTIVITIES AND RESPONSIBILITIES

"Be careful, the auditors are coming!" This was the kind of warning that was common in the not-too-distant past when an internal audit function announced to an enterprise manager that they had scheduled a review of an IT application, an overall IT-related

process, or some other area of interest. A typical IT process owner's first response here was that the planned audit was scheduled at a "bad time" for any of a variety of reasons. However, the planned internal audit would soon be scheduled, internal audit would perform their review, the results would be reported, and the manager would then be responsible for responding to any audit comments and implementing recommended corrective actions.

Senior managers need to understand the overall internal audit process and how internal audits are scheduled, performed, and then reported. While there can be many variations, depending on the size and complexity of an organization and the objectives of an audit, the typical internal audit process requires scheduling a review, performing a risk assessment and necessary audit procedures, and then reporting the results of an audit to management and the audit committee. Our goal is not to describe how to perform internal audits but to understand this general process. A key point here, however, is that the persons performing internal audits should not be acting as internal consultants. As discussed in our brief description of internal audit professional standards in the next section, the business executive who is not directly involved in the internal audit process should realize that the prime role of internal audit is to examine, review, and test internal controls and related processes. If internal audit is acting as an internal consultant, separate arrangements should be made such that all parties realize that internal consulting activities are separate and different from internal auditing.

The Internal Audit Process: Planning and Authorizing Internal Audits

Internal audit is not a separate function in a typical enterprise—such as purchasing, accounts receivable, or facility engineering. Rather, the internal audit function as well as the head of internal audit—normally the chief audit executive (CAE)—reports directly to the audit committee of the board of directors. In the United States, this requirement is mandated by the SEC. While internal audit may have a nominal reporting relationship to the CFO or some other administrative function, internal audit must have an independent relationship with the audit committee.

Internal audit activities are mandated through a formal internal audit charter document that has been approved by the audit committee and gives the internal audit function the overall authority to perform independent reviews and examine materials. From an IT governance perspective, for example, a charter document will give an internal audit team the authority to enter data center operations and to review otherwise secured reports and materials that are part of a planned audit.

Exhibit 19.1 is an example internal audit charter for the sample company, Global Computer Products, that has been used previously. It clearly outlines the "marching orders" for an internal audit organization. When an enterprise executive has questions about the activities and authority of their internal auditors, a copy of their charter should be requested. If it appears to miss some area, such as IT governance issues, or appears out of date, the CAE should be requested to start an audit charter update process.

EXHIBIT 19.1 Sample Internal Audit Charter

Global Computer Products

Internal Audit Department

Authorizing Charter

Internal Audit's Mission

The mission of Global Computer Products Internal Audit is to ensure that company operations follow high standards both by providing an independent, objective assurance function and by advising on best practice. By using a systematic and disciplined approach, Internal Audit helps Global Computer Products accomplish its objectives by evaluating and improving the effectiveness of risk management, internal control, and governance processes.

Independence and Objectivity

To ensure independence, Internal Audit reports directly to the Board of Directors Audit Committee, and to maintain objectivity, Internal Audit is not involved in day-to-day company operations or internal control procedures.

Scope and Responsibilities

The scope of Internal Audit's work includes the review of risk management procedures, internal control, IT systems, and governance processes. This work also involves periodic testing of transactions, best practice reviews, special investigations, appraisals of legal and regulatory requirements, and measures to help prevent and detect fraud.

To fulfill its responsibilities, Internal Audit shall:

__ Identify and assess potential risks to enterprise operations.
__ Review the adequacy of controls established to ensure compliance with policies, plans, procedures, and business objectives.
__ Assess the reliability and security of financial and management information and supporting systems and operations that produce this information.
__ Assess the means of safeguarding assets.
__ Review established processes and propose improvements.
__ Appraise the use of resources with regard to economy, efficiency, and effectiveness.
__ Follow up recommendations to make sure that effective remedial action is taken.
__ Carry out ad hoc appraisals, investigations, or reviews requested by the Audit Committee and Management.

Internal Audit's Authority

In order to promote effective controls at reasonable cost, Internal Audit is authorized, in the course of its activities, to:

__ Enter all areas of Global Computer Products operations and have access to any documents and records considered necessary for the performance of its functions.
__ Require all members of staff and Management to supply requested information and explanations within a reasonable period of time.

Accountability

Internal Audit shall prepare, in liaison with Management and the Audit Committee, an annual audit plan that is based on business risks, the results of other internal audits, and input from Management. The plan shall be presented to senior management, including the General Counsel, for approval by the Audit Committee. Any needed adjustments to the plan should be communicated to and approved by the Audit Committee.

(*continued*)

EXHIBIT 19.1 (*Continued*)

Internal Audit is responsible for planning, conducting, reporting, and following up on audit projects included in the audit plan, and deciding on the scope and timing of these audits. The results of each internal audit will be reported through a detailed audit report that summarizes the objectives and scope of the audit as well as observations and recommendations. In all cases, follow-up work will be undertaken to ensure adequate response to internal audit recommendations. Internal Audit also will submit an annual report to senior management and to the Audit Committee on the results of the audit work, including significant risk exposures and control issues.

Standards

Global Computer Products Internal Audit adheres to the standards and professional practices published by the Institute of Internal Auditors as well as the Information Technology Governance Institute.

While the audit committee may mandate or request that its CAE and internal audit function perform some specific internal audit review, internal audit—through its ongoing risk assessments, requests by other members of management, or its experiences with other internal audits—will typically develop short- and longer-range plans of the internal audits that it plans to perform over an upcoming period. Based on this plan, as well as recent past completed audits, the CAE should make arrangements for the internal audit staff and other resources to perform this program of planned enterprise internal audits.

The Internal Audit Process: Launching an Internal Audit

Exhibit 19.2 outlines the processes for performing an internal audit as four summarized phases or steps. Although an annual plan calls for an internal audit to be performed in some area, courtesy generally calls for internal audit to work with the area to be reviewed to gather some preliminary details about the area to be reviewed and to schedule the audit. Each phase on this exhibit outlines multiple activities. For example, the top-level phase calls for:

- **Schedule the audit.** After an overall annual audit plan has been established and approved by the audit committee, the specific audit should be scheduled, with consideration given to audit resource needs, auditee time resource considerations, and other factors.
- **Assign the auditors.** Resources are often scarce here. Care must be given to assigning IT audit specialists to appropriate assignments while internal auditors with other skills should be assigned where best suited.
- **Perform preliminary audit assessments.** Internal audit may schedule a review to assess the internal controls of some system or process, but before starting the actual audit, it is necessary to gather more information about the area to be reviewed and to make some preliminary assessments about the extent and depth of the area to be reviewed, its overall general internal controls and related risks, and approaches to test or assess the area to be audited.

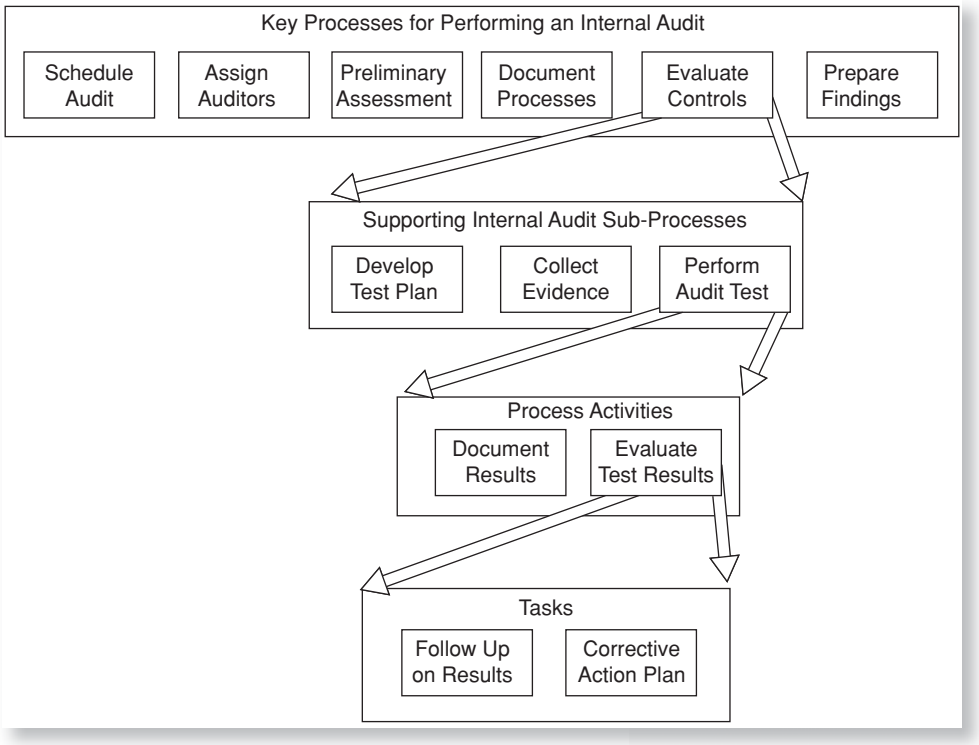

EXHIBIT 19.2 Process for Performing an Internal Audit

- **Document the processes for the area being audited.** Adequate documentation is a major requirement for all internal audit work. It is not sufficient to just say that some process has adequate internal controls; the internal auditor should gather documentary evidence to prove that those controls were adequate at the time of the auditor's review.
- **Evaluate the internal controls.** This is really the key to the internal audit process. An internal auditor takes an internal control being evaluated and develops a test plan to assess that process. This may involve collecting audit evidence, and performing audit tests, as shown in the next level of processes on the exhibit.
- **Prepare findings.** An internal auditor tests and evaluates internal controls through a variety of approaches, ranging from formal test of transactions to gaining impressions through interviews or from observations. Often called *internal audit findings,* these test results and observations may eventually find their way into a formal internal audit report outlining these audit findings and recommendations.

We have just described the basic steps in an internal audit process. An internal auditor will go through a similar pattern of these steps for each area to be reviewed. The goal of this chapter is not to describe to the senior executive how to perform an internal audit, but to give an understanding of the processes needed to perform an adequate internal audit. These basic steps will remain the same whether for a review of financial controls of some process or for a review of an IT system application.

The Internal Audit Process: Reviewing and Testing Audit Evidence

Much of the internal audit process requires gathering, reviewing, and testing what internal auditors call *audit evidence*. An internal auditor may ask about the status of the documentation for some new IT application and be told that the documentation is "up to date." If it is a minor system, the internal auditor might note that response and go forward. However, to have strong evidence that the documentation is up to date, the internal auditor might ask to see the actual documentation to determine that it exists. Going into more detail, an internal auditor might even dig into the documentation and check such things as the adequacy of revisions or perform other tests to see if that documentation is really adequate and supports system controls.

This whole process requires an internal auditor to assess the adequacy of the audit evidence found and make some assessments based on that internal audit work. Exhibit 19.3 shows various types of audit evidence ranging from the strongest to the weakest. The first column shows types of audit evidence, where an audit technique of actually observing some practice is much stronger than just being told. There is no requirement that all internal audit work should be supported by the strongest levels of evidence. The nature of the internal audit and associated risks are factors here, but a senior manager working with internal auditors and their recommendations should always consider how they gathered their audit evidence to support their documented conclusions.

The Internal Audit Process: Reporting Internal Audit Results

Internal audits should conclude with a formal report describing internal audit's review objectives in some area, what procedures were followed to assess internal controls for that audit objective, what was found, and whether the internal controls there were assessed as adequate or inadequate. In most instances, these audit reports will result in formal recommendations for internal control improvements based on the audit findings in the area reviewed. Although practices can vary across enterprises, internal audit reports will generally require a formal management response acknowledging internal audit's findings and stating how they will repair or correct the reported control deficiencies.

EXHIBIT 19.3 Internal Audit Strengths of Audit Evidence Classifications

Classifications of the Internal Audit Evidence Gathered	Evidence with Strongest Support for Audit Conclusions	Weakest Levels of Internal Audit Evidence
Audit Technique	Observations/Confirmation	Inquiry
Origin of Evidence	Corroborative	Underlying Statistics
Relationship to Auditee	External Department	Internal Group
Form of Evidence	Written/Secure System	Oral
Sophistication of Evidence	Formal/Documented	Informal
Location of Evidence	Created in Actual System	Derived from Support System
Source of Audit Evidence	Personal Audit Work	Supplied "Secondhand"

Audit reports are not for general distribution in an enterprise. They typically are directed only to the enterprise area that was reviewed and its direct managers, as well as to senior enterprise management, such as the CEO and CFO, the external audit partner, and the audit committee. An unfavorable audit finding in some area of operations really puts the focus on management to repair or correct internal control deficiencies in some area reviewed. It can be an important element of IT governance.

Internal auditors are typically faced with many areas to review and often lack the time and resources to adequately review all of the higher-risk areas in a large enterprise. For example, this author once was the internal audit director for a very large U.S. corporation with multiple operating units and had 3 unit audit managers and about 80 internal auditors on staff. Despite fairly extensive risk analyses and well-organized annual internal audit plans, it was difficult to complete all planned audits and cover all risks. Plans were regularly altered or adjusted because of new business crises that required additional audit activity. A newly discovered fraud activity, for example, might divert other internal audit activities to help better investigate the fraud allegation.

The reader seeking more information on internal auditing and its role in IT governance should refer to this author's previously mentioned book, *Brink's Modern Internal Auditing.* The book defines internal audit's common body of knowledge, the broad areas that an internal auditor should know or understand.

INTERNAL AUDIT IT GOVERNANCE STANDARDS

The internal auditor's professional organization, the IIA, is responsible for issuing standards of practice and conduct for all internal auditors, on essentially a worldwide basis. This authoritative guidance is a combination of mandatory standards statements that are required and necessary for the continued professional practice of auditing, plus a series of strongly recommended standards practices. These IIA standards go beyond just IT governance and cover internal audit governance activities on a broad basis. For example, the IIA Performance Standard 2110.A2 states:

> The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.

Although the standard is drafted in a very general manner, it essentially asks an internal auditor to assess whether an organization's IT infrastructure aligns and sustains business processes to properly manage the long-term goals for the overall enterprise.

INTERNAL AUDIT IT GOVERNANCE PROCEDURES

Based on our IT governance discussions of previous chapters, primary goals for IT governance are to assure that the investments in IT generate business value, and to

mitigate the risks that are associated with IT processes and systems. Many internal audit review activities can play a major role in supporting enterprise IT governance. An example here and a frequent IT internal audit activity is reviews and assessments of enterprise IT continuity plans, once called IT disaster recovery plans in the days of centralized mainframe systems. An enterprise IT function needs processes in place to restore operations and to recover IT resources to normal operating levels in the event of some long-term disruption in IT services. Internal audit reviews and assessments in this area very much support enterprise IT governance processes.

Internal audit can greatly support enterprise IT governance processes through review and assessments in these general areas. Exhibit 19.4 outlines five general areas where internal audit should focus in its reviews of IT governance: value delivery, risk management, resource management, performance management, and strategic alignment issues. Internal audit professional standards call for these levels of internal audit review activities:

- Review and assess the IT function's value delivery and how IT aligns with the organization's mission, vision, values, objectives, and strategies.
- Review whether the IT function has a clear statement about the performance expected by the business (effectiveness and efficiency) and assess its achievement.
- Review and assess the effectiveness of the IT resource and performance management processes.

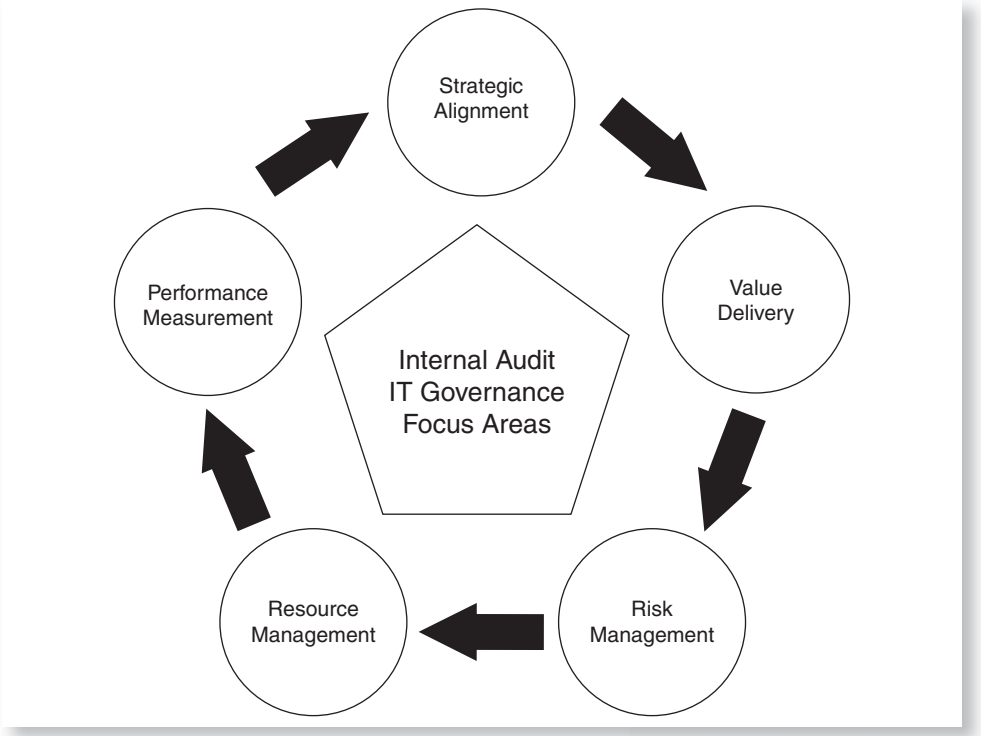

EXHIBIT 19.4 Internal Audit IT Governance Focus Areas

- Review and assess compliance with legal, environmental and information quality, and fiduciary and security requirements.
- Review and assess the control environment of the organization.
- Review and assess the risks that may adversely affect the IT environment.

Business executives who are not part of internal audit should realize and recognize that internal audit is an independent entity in an enterprise and that an executive who is not part of the audit committee cannot just direct internal audit to perform a review in some area. Their internal audit review plans should be established only through the approval of the audit committee. Nevertheless, enterprise executives in operations or IT management should feel free to ask their chief audit officer and other members of internal audit management about their plans and current activities in reviewing key areas of enterprise IT governance.

Internal Audit Reviews of IT Strategic Alignment Processes

As part of an enterprise IT organization's annual plans and ongoing activities, internal audit should assess whether those IT plans and operations mesh with other enterprise business activities. A key component of this is that all IT operations, including systems development, quality management, and IT processing, should be aligned with business operations. That is, IT operations should add value and competitive positioning to an enterprise's products and services. An IT function should strive to maintain its costs through improving administrative efficiency and managerial effectiveness. While these are all IT and general management calls, an internal audit function should always raise and ask some hard questions in the course of its reviews.

As mentioned earlier, an effective IT function should have some type of steering committee, long-range planning function where a representative mix of users of IT resources can meet with IT management and review or approve new proposals and set priorities on new efforts. IT audit should recommend that such an effective function be in place and often should sit in as a participant to steering committee meetings. The steering committee should establish a long-range strategy for IT activities and investments, and periodic internal audit reviews—through passive participation in steering committee sessions or formal internal audit reviews—should ensure that this IT strategy is in place and is operational.

There should be an integrated approach to the enterprise business and IT strategy, with co-responsibility assignments to both. In addition, although IT functions are sometimes guilty of adopting new and untried approaches, there should be clearly stated objectives for these efforts. Internal audit can be an effective voice through its reviews and audit comments in helping to assure that these objectives are met.

Internal Audit Reviews of IT Value Delivery Processes

Internal audit reviews should be tailored to ensure that IT continues to deliver its promised benefits against its stated strategies. The idea here is that new IT projects, whether for new or improved application processes or new hardware tools, are proposed to include expected benefits. While certainly internal audit will not be able to review all

of these efforts, due to priority and resource limitations, it should periodically assess stated benefits to find if stated goals are being achieved. Internal audit should look for formal return on investment, total cost of ownership, and facilities to measure IT efforts.

As discussed in Chapter 16 on project management, the enterprise IT function should have a formal IT project management process in place to deliver benefits to business operations. Assessing value delivery goes beyond more traditional internal audits that focus on internal controls and looks for greater value delivery in IT operations. There is a need for a formal commitment to installing formal methodologies for the overall development of IT service delivery.

This concept of internal audit reviews of IT service delivery processes goes beyond many traditional internal audit review efforts. Chapter 6 discussed IT service delivery as part of ITIL concepts and IT service management. An effective internal audit function needs to understand these concepts and meld them into other internal audit procedures.

Internal Audit Reviews of IT Risk Management Processes

As has been emphasized in Chapter 8 on risk management and in other comments throughout these chapters, risk management is a very important IT governance concept, and an appreciation and understanding of it should be part of virtually all internal audit reviews. This requires an awareness by senior officers of the enterprise's appetite for risk. IT risk management responsibilities should be embedded into all levels of business operations. This area is often a concern with IT operations where there have been historical tendencies to try new systems approaches or technologies with little understanding of any associated risks. While IT management and the users of IT should be the ones responsible here, there is often a tendency to try some new and untested approach with little thought to the risks if it fails. Internal audit can often be very effective in raising hard devil's-advocate questions as part of its reviews.

Appropriate risk management processes should emphasize the safeguarding of IT assets and supporting systems through disaster recovery procedures and effective plans for the continuity of operations. This has been a traditional area for internal audit and IT audit reviews and should be emphasized as part of a review of IT governance activities.

All internal audit reviews should focus on an awareness of IT risks based on a transparency to all stakeholders and should make efforts to embed risk management as an integral part of enterprise compliance and assurance. This really says that an internal audit function should go beyond just its specialized IT audit reviews and add IT risk management concerns to all reviews covering areas of IT governance. In addition to overall internal audits, there is a need to establish effective process management assessments as part of internal audit reviews.

Internal Audit Reviews of IT Resource Management Processes

IT internal audit should regularly review and assess the effectiveness of its IT resource and performance management processes. In many enterprises, IT facilities and operations represent one of the major—if not *the* major—requirements for enterprise resources. Management should invest in these IT resources through formal long-range project plans and established budgeting processes. Other chapters

have covered IT resource management issues from the perspective of overall business operations. For example, Chapter 14 discusses the importance of IT configuration and portfolio management as a means to better manage and control diverse IT assets. Similarly, Chapter 17 discusses service level agreements as a means of maximizing the value of business investments.

Internal audit should plan and develop a series of reviews in these areas of IT resource management. This said, it is difficult for an internal audit function to just launch a review of IT resource management, as the topic and area is almost too broad for a single internal audit review. Rather, internal audit should develop and perform specialized reviews in many if not all of the areas of IT governance discussed in these chapters.

Internal Audit Reviews of IT Performance Measurement Processes

Performance measurement techniques should be developed to help translate strategies into actions in order to achieve and measure IT goal achievements. This type of tool can measure the relationships and assets necessary to achieve a customer focus, process efficiencies, and facilities to help the overall enterprise and its IT functions to learn and grow. These types of tools track project delivery and monitor IT services.

Exhibit 19.5 summarizes the types of internal audit review and assessment activities necessary to promote IT governance in an enterprise. The exhibit is at a very high level but emphasizes that internal auditors need to review IT systems and operations to help optimize overall enterprise internal control processes, to simplify and improve these processes, to recommend areas for better automation, and to suggest areas for better systems and process standardization. These internal audit review areas cover a

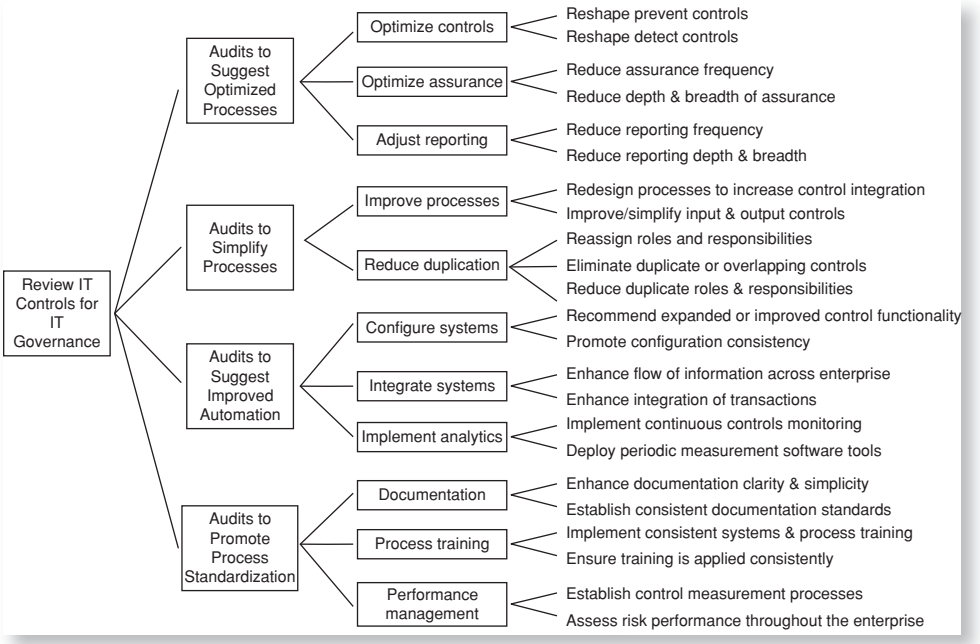

EXHIBIT 19.5 IT Governance IT Audit Review Activities

wide range of audit activities that are beyond the internal audit comments summarized earlier in this chapter and are part of internal audit's best practices and common body of knowledge needs. An effective internal audit function should be a key component in promoting effective IT governance processes in any enterprise.

NOTE

1. Now in its seventh edition, *Brink's Modern Internal Auditing* is published by John Wiley & Sons, with Robert R. Moeller as the author.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

PART SIX

VI

IT Governance and Enterprise Objectives

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER TWENTY

Creating and Sustaining an Ethical Workplace Culture

AS DISCUSSED IN PREVIOUS CHAPTERS, IT governance processes should be integrated into the core operations of an enterprise's business as well as where the management of each subsidiary or business unit is responsible for ensuring proper IT governance processes. As an element of this, an enterprise must be committed to achieving the highest standards of ethics and integrity in all aspects of its business operation. The integrity of an enterprise should begin with every stakeholder's and employee's commitment to the enterprise's core values and their responsibility to act in concert with those values.

This chapter discusses the importance of enterprise ethics and governance policies, oversight structures, and processes, including steps for establishing an effective ethics function, developing and implementing effective codes of conduct, and establishing an effective enterprise compliance committee under the board of directors. Our objective is to outline some best practices that an enterprise can use and implement to establish an ethical workplace culture.

The issues and best practices discussed in this chapter go beyond just IT and IT governance operations and extend to all aspects of the enterprise. However, best practices such as an effective enterprise code of conduct and a senior management–supported mission statement should gain the support of all enterprise stakeholders. The result should be an ethical workplace culture.

IMPORTANCE OF MISSION STATEMENTS

Previous chapters have discussed many important IT governance issues, and most have emphasized the need to establish effective IT governance standards and processes, such as Chapter 7 on ISO governance standards or Chapter 12 on IT operations service

catalogs. Each of these emphasizes specific areas to improve enterprise IT operations. However, an effective enterprise mission statement, covering all aspects of operations and all stakeholders, should be a key element in establishing effective IT governance practices.

Every enterprise, no matter how big or small, needs a mission statement to describe its overall objectives and values. It should be a source of direction—a compass—letting employees, customers, stockholders, and other stakeholders know what the enterprise stands for and what it does not. While in years past a mission statement was often little more than a nice but tired-sounding slogan, an effective enterprise mission statement today should be a very important element in any program of management ethics and good corporate governance. Effective mission statements can be a great asset to an enterprise, allowing it to better achieve its overall goals and purposes.

Although it is years ago now, the Johnson & Johnson Tylenol crisis of the early 1980s provides a good example of the importance of a strong corporate mission statement acting as a compass to provide direction. Johnson & Johnson, a major medical products provider, manufactured a popular over-the-counter pain reliever medication called Tylenol. In those days, such medications were sold in screw-top bottles. Someone in the Chicago area opened a series of these Tylenol bottles, adulterated their contents with cyanide, and replaced the bottles on store shelves. Several people who purchased this tainted Tylenol subsequently died from poisoning. An investigation of these deaths quickly pointed to Johnson & Johnson and the cyanide-tainted Tylenol.

This whole matter put Johnson & Johnson under massive pressure. The corporation knew that it had extremely strong quality-control processes in place that would prevent such poison contamination from occurring within its own manufacturing facilities. The company also knew that the contaminated products had appeared only in the Chicago area, while Tylenol was found on store shelves worldwide. A total product recall would be extremely expensive. However, Johnson & Johnson did not go through a long series of internal investigations and quickly did the right thing. It recalled all of its Tylenol products from store shelves worldwide and subsequently rereleased them in a newly designed sealed package. When asked why it made such a very expensive recall decision so quickly with no evidence that it was at fault, the corporation stated that there was no need for a delayed decision. The Johnson & Johnson Credo, its mission statement, dictated that decision. That Johnson & Johnson Credo states very strongly that the company's first responsibility is to supply high-quality products to its customers. The credo can be found on the Johnson & Johnson Web site, and is shown in Exhibit 20.1. At the time of the Tylenol crisis, everyone at Johnson & Johnson knew this, the credo had been posted widely in enterprise facilities, and there was no need for a decision. The whole unfortunate matter really highlighted the importance of a strong mission statement for an enterprise.

A strong corporate mission statement is an important element in any ethics and corporate governance initiative. Although most enterprises will not face a crisis on the level of Johnson & Johnson with its tainted Tylenol in the 1980s, a stronger anchor of

EXHIBIT 20.1 Johnson & Johnson Credo or Mission Statement

Our Credo (As published in JnJ.com)

We believe our first responsibility is to the doctors, nurses and patients,
to mothers and fathers and all others who use our products and services.
In meeting their needs everything we do must be of high quality.
We must constantly strive to reduce our costs
in order to maintain reasonable prices.
Customers' orders must be serviced promptly and accurately.
Our suppliers and distributors must have an opportunity
to make a fair profit.

We are responsible to our employees,
the men and women who work with us throughout the world.
Everyone must be considered as an individual.
We must respect their dignity and recognize their merit.
They must have a sense of security in their jobs.
Compensation must be fair and adequate,
and working conditions clean, orderly and safe.
We must be mindful of ways to help our employees fulfill
their family responsibilities.
Employees must feel free to make suggestions and complaints.
There must be equal opportunity for employment, development
and advancement for those qualified.
We must provide competent management,
and their actions must be just and ethical.

We are responsible to the communities in which we live and work
and to the world community as well.
We must be good citizens—support good works and charities
and bear our fair share of taxes.
We must encourage civic improvements and better health and education.
We must maintain in good order
the property we are privileged to use,
protecting the environment and natural resources.

Our final responsibility is to our stockholders.
Business must make a sound profit.
We must experiment with new ideas.
Research must be carried on, innovative programs developed
and mistakes paid for.
New equipment must be purchased, new facilities provided
and new products launched.
Reserves must be created to provide for adverse times.
When we operate according to these principles,
the stockholders should realize a fair return.

Source: Johnson & Johnson

this sort might have helped some enterprises to better avoid the accounting scandals in recent years that led to the Sarbanes-Oxley Act (SOx) as highlighted in Chapter 2.

Enterprise management should evaluate any mission statement that may exist today or consider rewriting and launching a new one if needed. If employees or other stakeholders are not aware of any existing corporate mission statement or if they view it with little more than cynicism, there is a need to revisit and revise that document. A poorly crafted mission statement can often do more harm than good, creating cynical and unhappy organization members who resist change. If the enterprise has no mission or values statement, there can be considerable value to assembling a team to develop a statement that reflects the enterprise's overall values and purposes. If an existing mission statement is met with cynicism during a stakeholder survey, it is time to carefully craft and revise that statement. However, if just rolled out with no preparation, it may be viewed with even more cynicism. A good mission statement also is a good starting point for the corporate "tone at the top" message for today's corporation, as discussed in Chapter 2.

A good mission statement should make a positive statement about a corporation; it should hopefully inspire organization members to harness their energy and passion and increase their commitment to achieving goals and objectives. The idea is to create a sense of purpose and direction that will be shared throughout the enterprise. Again going back many years ago, perhaps one of the best examples of a mission statement was expressed by U.S. president John F. Kennedy in the early 1960s:

> This nation should dedicate itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to Earth.

Those simple words describe a mission and vision much better than an extensive document of many pages. Sometimes called *values statements* or *credos,* these statements can also be found in many enterprises' annual reports. Some are lengthy, while others seem to be little more than fluff. The best are closer to the Johnson & Johnson credo or the moon landing statement in their style.

Once an enterprise has developed a new mission statement or has revised an existing one, it should be rolled out to all enterprise members with a good level of publicity. Using a tone-at-the-top approach, senior managers should explain the reasons for the new mission statement and why it will be important for the enterprise. It should be posted on facility billboards, in the annual report, and in other places to encourage all stakeholders to understand and accept it. That mission statement should not just stand by itself. A series of other key steps are needed to build an effective ethics and compliance function, starting with surveys and other mechanisms.

ENTERPRISE CODES OF CONDUCT

While a strong and effective mission statement is a key element in the overall structure of corporate governance, the code of conduct provides the supporting rules for enterprise stakeholders. These codes have been common in major corporations for

many years, and SOx now requires that corporations must develop a code of ethics for their senior financial officers. While this SOx code is mandated, all enterprises can benefit from a code of conduct that covers all stakeholders. While SOx uses the expression "code of ethics," we refer to it here by perhaps its more common name, the *enterprise code of conduct*.

An enterprise today should develop and enforce a code of conduct that covers a set of appropriate ethical, business, and legal rules for all enterprise stakeholders, including senior management, all staff and supervisory employees, and its larger group stakeholders. Enterprise senior management should assemble a team of unit operations and financial managers, representatives for internal audit and quality assurance, corporate communications, human resources, and certainly corporate legal to build or reconstruct an effective code of conduct that promotes ethical business practices throughout the enterprise.

The Contents: What Should Be the Code's Message?

A code of conduct should be a clear, unambiguous set of rules or guidance that outlines what is expected of members of the enterprise, whether officers, employees, contractors, vendors, or any other stakeholders. The code should be based on the values and legal issues surrounding an enterprise. That is, while all enterprises can expect to have code of conduct prohibitions against sexual and racial discrimination, a defense contractor with many contract-related rules issues will have a somewhat different code of conduct than a fast-food operation. However, any such code should apply to all members of the enterprise from the most senior level to a part-time clerical employee. For example, a code of conduct rule prohibiting erroneous financial reporting should be the same whether directed at the CFO for incorrect financial reporting or the part-timer for an incorrect or fraudulent weekly time card.

If the enterprise already has a code of conduct, enterprise management should consider revising or refreshing it as appropriate. All too often, older codes were originally drafted as rules for the lower-level employees, with little attention given to the more senior members of the enterprise. An effective code of conduct should be delivered in a manner that will apply to all enterprise stakeholders, with an almost greater emphasis today on enterprise senior officers. Working with senior members of management and the audit committee, a selected management team should examine any existing code of conduct to determine whether its rules and guidance still fit the enterprise governance and post-SOx era of today.

Whether for a revision to an existing code of conduct or the development of a new code, a joint team from a cross section of management should be assembled for such a task. The team should examine the business issues facing the enterprise and then draft a set of code rules that are applicable to that enterprise depending on their business and related issues. The code rules must be written in a clear manner such that the points can be easily understood by all. Exhibit 20.2 lists some example code of conduct topics. While this list does not apply to all, these topics are appropriate for many modern enterprises today. The key is that messages delivered in the code must be clear and unambiguous. This author was very involved in drafting a code of conduct for a large U.S. corporation

EXHIBIT 20.2 Example Code of Conduct Topics

The following are topics found in a typical enterprise code of conduct

I. INTRODUCTION

A. Purpose of This Code of Conduct: A general statement about the background of this Code of Conduct.

B. Our Commitment to Strong Ethical Standards: A restatement of the Mission Statement along with a printed letter from the CEO.

C. Where to Seek Guidance: A description of the enterprise ethics hotline process.

D. Reporting Noncompliance: Guidance for whistleblowers—how to report.

E. Your Responsibility to Acknowledge the Code: A description of the code acknowledgment process.

II. FAIR DEALING

A. Our Selling Practice: Guidance for dealing with customers.

B. Our Buying Practices: Guidance and policies for dealing with vendors.

III. CONDUCT IN THE WORKPLACE

A. Equal Employment Opportunity Standards: A strong commitment statement.

B. Workplace and Sexual Harassment: An equally strong commitment statement.

C. Alcohol and Substance Abuse: A policy statement in this area.

IV. CONFLICTS OF INTEREST

A. Outside Employment: Limitations on accepting employment from competitors.

B. Personal Investments: Rules regarding using company data to make personal investment decisions.

C. Gifts and Other Benefits: Rules regarding receiving bribes and improper gifts.

D. Former Employees: Rules prohibiting giving favors to ex-employees in business.

E. Family Members: Rules about giving business to family members, creating potential conflicts of interest.

V. COMPANY PROPERTY AND RECORDS

A. Company Assets: A strong statement on the employees' responsibility to protect assets.

B. Computer Systems Resources: An expansion of the company assets statement to reflect all aspects of computer systems resources.

C. Use of the Company's Name: A rule that the company name should only be used for normal business dealings.

D. Company Records: A rule regarding employee responsibility for records integrity.

E. Confidential Information: Rules on the importance of keeping all company information confidential and not disclosing it to outsiders.

F. Employee Privacy: A strong statement on the importance of keeping employee personal information confidential and not disclosing it to outsiders and even other employees.

G. Company Benefits: Employees must not take company benefits where they are not entitled.

(*Continued*)

EXHIBIT 20.2 (*Continued*)

VI. COMPLYING WITH THE LAW

A. Inside Information and Insider Trading: A strong rule prohibiting insider trading or otherwise benefiting from inside information.

B. Political Contributions and Activities: A strong statement on political activity rules.

C. Bribery and Kickbacks: A firm rule on accepting bribes or kickbacks.

D. Foreign Business Dealings: Rules regarding dealing with foreign agents in line with the Foreign Corrupt Practices Act.

E. Workplace Safety: A statement on the company policy to comply with OSHA rules.

F. Product Safety: A statement on the company commitment to product safety.

G. Environmental Protection: A rule regarding the company's commitment to comply with applicable environmental laws.

several years ago. The following example is an extract from that code of conduct on a section covering company assets:

> We all have a responsibility to care for all of the company's assets including inventory, cash, supplies, facilities, and the services of other employees and computer systems resources. If you see or suspect that another employee is stealing, engaging in fraudulent activities, or otherwise not properly protecting company assets, you may report these activities to your manager or to the ethics office.

These words are a good example of the tone and style of a good code of conduct. It places the responsibility on the recipient of the code, tries to explain the issues in an unambiguous manner, and suggests expected responses and actions.

In addition to the code topics as well as the code rules, many enterprises have found value in adding a set of questions and answers to accompany the points in the code. This allows the code's reader to better understand the issues as well as the types of questions that a perhaps more unsophisticated employee might ask regarding a code rule. The key to a clear set of code of conduct rules is that they must be clear and understood by all. This can be a real editing challenge for the code of conduct team.

We have not included sample codes of conduct in this book, as the codes of conduct for almost every enterprise look different in terms of style, format, and size. Some enterprises publish rather elaborate documents, while others are very bare-bones. Enterprise codes of conduct, by their nature, are certainly not company trade secrets, and calls to a corporate information or public relations office will typically garner sample copies of their code of conduct.

Global corporations have another issue when developing a code of conduct. Although a corporation may be headquartered in the United States, it may have significant operations worldwide where key managers, employees, and other stakeholders do not use English as their primary language. Although there will be the added costs of translation, consideration should be given to producing a version of the code of conduct in at least the major languages used in corporate operations. If there are many locations but only small numbers of foreign-language stakeholders, a summary of the main code

of conduct in each of the local languages might be appropriate. However, those summary versions should certainly emphasize the same SOA financial fraud guidance that is contained in the primary code of conduct.

Code of Conduct Communications to Stakeholders to Assure Compliance

An enterprise's code of conduct must be a *living document*. It has little value if it has merely been developed, delivered to all stakeholders with much hullabaloo, and then filed away and forgotten. With a new code of conduct or even a major revision of the existing code, the enterprise should undertake a major effort to deliver a copy of that code of conduct to all employees and stakeholders. A good first step would be to formally present that new or revised code of conduct to the enterprise's senior executives, and particularly the financial officers. Codes of conduct in the past sometimes received only token acceptance from the senior officer group, with a feeling that it was really for the staff and not for them. The reported financial scandals leading up to the enactment of SOx in the early years of this century really highlighted this discrepancy. Both Enron and WorldCom,[1] two oft-cited "bad guys" of that pre-SOx era, had adequate corporate codes of conduct. However, their corporate officers did not seem to feel that the rules applied to them.

A disturbing example of a lack of high-level corporate officer code of conduct acceptance can be found in the former Enron CFO, Andrew Fastow. Because he knew that he would be violating the Enron corporate code of conduct with some questionable off-balance-sheet accounting schemes, Fastow went to the Enron audit committee and asked it to formally vote him an exemption from the code of conduct rules! The audit committee *granted* this exemption, one more step in the ultimate failure of Enron.

Enterprise senior managers should formally acknowledge that they have read, understand, and will abide by the code of conduct. With the management team standing behind it, the enterprise should next roll out and deliver the code of conduct to all stakeholders in the enterprise. This can be done in multiple phases, with delivery to local or more major facilities first, followed by smaller units, foreign locations, and other stakeholders. Rather than just including a copy of the code with payroll documents, an enterprise should make a formal effort to present the code in a manner that will gain attention.

The new code can be communicated through such methods as a Webinar led by the CEO, training sessions, or other means to communicate its importance and meaning. Special communication methods might be used for other groups such as vendors or contractors, but an enterprise objective should be to get all stakeholders to formally acknowledge that they will abide by the enterprise's code of conduct. This can be accomplished by an Internet or telephone-response type of system where every enterprise stakeholder is asked to respond to these three questions:

1. Have you received and read a copy of the code of conduct? Answer yes or no.
2. Do you understand the contents of the code of conduct? Answer yes if you understand this code of conduct or no if you have questions.
3. Do you agree to abide by the policies and guidelines in this code of conduct? Answer yes if you agree to abide by the code and no if you do not.

The whole idea is to require every employee and stakeholder to acknowledge acceptance of the enterprise's code of conduct. Responses should be recorded on some form of computer database listing the employee name and the date of their review and acceptance or nonacceptance. Any issues arising from question 2 can be handled through the whistleblower program described later. The idea is to have everyone—all of the stakeholders—buy into the code of conduct concept and agree to its terms. If someone refuses to accept the code because of questions, supervisors or others should discuss the matter with that person to gain eventual resolution. The final issue here is that the enterprise should expect all employees to agree to accept and abide by the enterprise's code of conduct. Following that code of conduct is just another work rule, and consistent failure to abide by these rules should be grounds for termination.

The whole concept behind this code acknowledgment requirement is to avoid any "I didn't know that was the rule" excuses in the future when code violations are encountered. It is a good idea to go through this code acceptance process on an annual basis or at least after any revision to the code document. The files documenting these code acknowledgments should be retained in a secure manner.

Code Violations and Corrective Actions

A code of conduct lays out a set of rules for expected behavior in an enterprise, in the form of guidance for all stakeholders—the financial officers as well as all others, including employees at all levels, contractors, and vendors. In addition to publishing its code of conduct and obtaining stakeholder acceptance to the code, there is a need for a mechanism to report code violations and for investigating and handling those violations.

The objective is that if an enterprise issues a strong code of conduct along with a message from the CEO about the importance of good ethical practices, all stakeholders should be expected to follow those rules. However, we all know that people are people and there will always be some who violate the rules or run on the edge. An enterprise needs to establish a mechanism to allow employees or even outsiders to report potential violations of the code in a secure and confidential manner. Much of that reporting mechanism can be handled through an ethics hotline or whistleblower facility as discussed in the next section. Other potential violations must be handled on a different level. Consider the male supervisor who hints that sexual favors from a female employee might be a good way to advance in the enterprise. A code of conduct sexual harassment prohibition will not necessarily stop the supervisor, and the employee often cannot easily go to a manager one level above the supervisor to report the situation. A process should be established for reporting all types of ethics violations.

An enterprise code of conduct should be supported with documented planned actions and responses for violations. When significant code infractions or violations are reported or found, the matter should be investigated and actions taken on a consistent basis, no matter the rank of the enterprise stakeholders responsible for the code violation. If the code of conduct prohibits making copies of corporate software—and it should—the penalties for a staff analyst in a remote sales office or a senior manager in corporate headquarters should be the same. Assuming they both have read the

prohibition in the code and acknowledged acceptance, penalties for violations should be consistent. Otherwise, there can be an atmosphere where the rules appear to apply only to some.

Most code of conduct violations can be handled through the enterprise's normal human resources procedures that probably have some process where there may be verbal counseling or probation for a first offense and leading to termination if there is a reoccurrence. Some matters that appear to be civil, or even potential criminal, violations must be reported to outside authorities and the matter then moves out of the enterprise's hands. The overall goal is that the enterprise must have some process in place to encourage all stakeholders to follow good ethical practices, as defined in the code of conduct, and to provide a consistent mechanism for reporting violations and taking disciplinary action when necessary.

Keeping the Code Current

Many of the basic rules of good ethical behavior as well as basic enterprise rules will not change from year to year. The example rule about protection of company assets, cited previously, stated that all stakeholders had a responsibility to care for their enterprise's assets, whether property, cash, computer resources, or others. That type of ethical rule will not change over time, whereas others may change due to business or other conditions. This author directed the internal audit function for a large retail enterprise—we will call it Company A—that originally had a code of conduct rule prohibiting employees from working for competitors. That was appropriate when a shopping mall salesperson worked for Company A full time. However, in our current era of much part-time work, it was not appropriate to tell a half-time shopping mall salesperson that he or she could not work part time for another retailer, Company B, in the same shopping mall. The code of conduct rule here was changed to state that while on the job for Company A, the employee's loyalty had to be with A and not B.

Enterprises should review their published codes of conduct on a periodic basis and at least every two years make certain that the guidance is still applicable and current. Changes to the code of conduct should not be treated lightly. Any revision should go through the same announcement and rollout process that was used for code introductions. The revised code should be issued to all stakeholders along with an explanation of the changes and a requirement to reacknowledge acceptance, as discussed previously.

As new employees and other stakeholders join the enterprise, they should be given the existing code of conduct, with the same requirement that they read and affirm the document. Consideration might be given to an online video to explain and educate new employees regarding the code of conduct and the enterprise's commitment to it. Also, whether the code is revised or not, all stakeholders should be asked, on a periodic basis, to reaffirm that they have read and will continue to abide by the code.

A new code of conduct revision and request for stakeholder reaffirmation can be an expensive task requiring dedicated enterprise resources from the ethics function, human resources, internal audit, and others. Along with the mission statement, an enterprise should keep its code of conduct and supporting principles in front of all stakeholders at all times. This can be accomplished through constant references to the code

of conduct such as in bulletin board posters in all facilities, instructive questions and answers in publications, or segments in employee training classes.

WHISTLEBLOWER AND HOTLINE FUNCTIONS

Whistleblowing is an important element or concept of corporate governance. A whistleblower is a person who tells the public or someone in authority about alleged dishonest or illegal activities occurring in a government department or private or public enterprise. This alleged misconduct may be a violation of a law, rule, or regulation and/or a direct threat to the public interest, such as fraud, health/safety violations, or corruption. Whistleblowers may make their allegations internally to other people within their enterprise or externally to regulators, law enforcement agencies, the media, or groups concerned with the issues.

Whistleblower programs have been around for some years to support federal contracting laws, health and safety regulations, and others. As highlighted in Chapter 2, SOx mandates that enterprise audit committees establish procedures to "handle whistleblower information regarding questionable accounting or auditing matters." When these SOx rules were first becoming active, there was much speculation that this SOx whistleblower provision would become a litigation nightmare for many U.S. corporations, with many employees filing whistleblower claims. This has not happened to date, and at the time of our publication there have been few recorded SOx whistleblower complaints filed and even fewer settlement actions. The legal process has proven to be a difficult way to resolve and settle issues.

Nevertheless, an enterprise facility needs to recognize and deal with whistleblower allegations as an important element of corporate governance. An enterprise should install an internal support function where a stakeholder can report any suspected concerns anonymously and can expect appropriate remedial actions. Based on our experience in setting up such a function for a major U.S. corporation, we call this type of facility an ethics hotline.

An enterprise ethics hotline function should be a 24/7 facility where any employee or stakeholder who sees some form of wrongdoing can independently and anonymously report that action with no fear of retribution. The matter can be reported to the organization or to regulatory authorities. There should be no retribution against the employee or legal action initiated to recover damages. Such whistleblower allegations can inflict serious damage on an organization's reputation as well as on the careers of accused managers. While SOx rules require the audit committee to establish a whistleblower facility, other enterprise functions, such as human resources, internal audit, or an ethics department, will need to actually set things up.

The SOx-mandated whistleblower program throws a challenge to audit committee members. The typical board of directors audit committee member *may* be aware of the needs for an effective whistleblower program, but almost certainly will not be aware of the necessary processes to establish one. Internal audit groups or human resources can often help the audit committee to establish an effective whistleblower program that will comply with SOx requirements. Effective whistleblower programs are one of those

concepts that many executives have heard about but may not fully understand. The following sections provide more information on them.

Federal Whistleblower Rules

The U.S. Department of Labor (DOL) administers and enforces more than 200 federal laws covering many workplace activities for about 10 million employers and 125 million workers. Most labor and public safety laws and many environmental laws mandate whistleblower protections for employees who report violations of the law by their employers. The SOx whistleblower rules apply to all employees of SEC-registered organizations, and public companies should pay special attention to these protections for corporate whistleblowers. SOx mandates whistleblower protection for stakeholders of publicly traded companies, allowing that no public company or any officer, employee, contractor, or agent of such company "may discharge, demote, suspend, threaten, harass, or in any other manner discriminate against an employee in the terms and conditions of employment because of any lawful act done by the employee." Those lawful acts are when the employee provides information or otherwise assists in an investigation conducted by a federal regulatory or law enforcement agency, Congress, or company personnel regarding any conduct that the employee "reasonably believes" constitutes a violation of SEC rules and regulations, fraud statutes, or files, testifies, participates in, or otherwise assists in a proceeding—pending or about to be filed—relating to an alleged violation. In other words, the employee or stakeholder who perceives some financial wrongdoing and then reports the matter is legally protected during its investigation and resolution.

In many respects, whistleblower provisions are primarily designed to protect employees who think they have discovered some wrongdoing rather than to increase organization internal controls. Virtually any personnel action taken against a whistleblower employee, including a demotion or suspension, can potentially be subject to legal action under this provision. Although there has been only limited SOx-related whistleblower experience at this time, the SEC and DOL are two federal agencies that can be expected to broadly protect accounting and auditing whistleblower employees. This says that an employee or stakeholder who registers a whistleblower complaint will be protected until the matter is resolved.

Under SOx, it is a crime for anyone "knowingly, with the intent to retaliate," to interfere with the employment or livelihood of any person—a whistleblower—who provides a law enforcement officer any truthful information relating to the possible commission of a SOx violation offense. Any whistleblower employee who thereby faces adverse employment action could potentially become a "protected informant" witness.

SOx requires the audit committees to establish a process for the receipt and treatment of complaints received regarding accounting, internal accounting controls, or auditing matters, and for "the confidential, anonymous submission by employees" regarding questionable accounting or auditing matters. Stakeholders who believe they have been unlawfully discharged or discriminated against due to their whistleblower action may seek relief by filing a complaint with the DOL or initiating federal district court action. The aggrieved will typically need to secure legal help to seek relief, and the process can be time-consuming and expensive for both the whistleblower and the

corporation that has been accused of the violation. For example, to prevail on a complaint before DOL, the employee must demonstrate that discriminatory reasons were a "contributing factor" in the unfavorable personnel action. Relief will be denied, however, if the employer demonstrates by "clear and convincing evidence" that it would have taken the same personnel action in the absence of protected activity.

An employee prevailing in such an action is entitled to full compensatory damages, including reinstatement, back pay with interest, and compensation for the litigation costs and attorney fees. Complicating matters further, the harmed whistleblower can take action on several fronts, seeking protection under federal and state laws as well as any collective bargaining agreement. Employers are exposed to potential double jeopardy for whistleblower actions, with liability under SOx provisions as well as state or federal laws on wrongful discharge and similar causes of action. In addition, the aggrieved whistleblower can seek punitive damages through separate court actions.

Judging by past administrative and judicial experiences in the nuclear energy and the airlines industries, whistleblower protection laws can become a potential minefield for corporations. If an employee raises any sort of accounting or auditing assertion regarding an improper or illegal act, that whistleblower is totally protected until the matter is investigated and resolved. There will be lots of trial lawyers in the wings eager to help the whistleblower and to file actions, particularly against major corporations with deep pockets. In addition, a substantial body of DOL and court precedent exists in this area to support regulatory sanctions and personal remedies.

From the perspective of over 20 years of experience with SOx whistleblower activities in the United States, an impacted organization should attempt to strike a balance between the rights of employees to raise whistleblower concerns and the ability to manage the workforce. A positive work environment is needed in which employees feel free to raise concerns to management coupled with effective mechanisms to deal with any concerns raised. The strong ethics-related programs discussed in the first sections of this chapter are important to establish an environment that hopefully limits whistleblower activities.

Whistleblower Rules and Enterprise Controls

Using SOx rules as an example, any employee or other stakeholder can become a whistleblower by reporting an illegal or improper activity covering accounting, internal control, and auditing. This should be an effective process when the potential whistleblower is a member of the corporate accounting staff who hears of plans for some fraudulent transactions or an employee at a remote unit that is not frequently visited by corporate staff, such as internal audit. Whistleblower rules are designed to encourage stakeholders to report these fraudulent or illegal acts and to very much protect the person who reported the matter. This raises a series of issues regarding internal auditors and internal audit reviews in particular.

An objective of internal auditing, discussed in Chapter 19, is to review and discover internal control problems and auditing issues. Internal audit findings are reviewed with management and presented in a formal audit report where management can outline its plans for corrective action. However, what if the internal audit team discovers an

accounting, internal control, or auditing matter that is not formally reported to management in the audit report? Can one of the audit team members independently report the matter under whistleblower procedures? Can an internal auditor who encounters an accounting and internal control matter that is not part of a scheduled audit go through the whistleblower protection route to report the matter? What if the internal audit team member has not been performing well and fears termination? Can that shaky-status auditor dig up some potential findings, perhaps from past workpapers, and report them outside of the audit department to obtain whistleblower protection and job security until the matter is resolved?

The internal audit team is clearly part of management, and internal auditors have a first responsibility to report any improper or illegal matters encountered during an audit to internal audit management for disposition. Internal audit team members should not attempt to work as independent whistleblowers as part of their internal audit work. Internal audit should develop a clear policy stating that any accounting, internal control, or auditing matters encountered during the course of a scheduled audit review should be documented in the audit workpapers and communicated to internal audit management for resolution. Both the internal audit team and the management of the functions audited should understand that the purpose of internal audit is not to let loose a team of potential whistleblowers in a department's books and records. Any illegal or improper items should be investigated and reported through the normal internal audit process.

A situation could exist where an internal auditor finds that some accounting or internal control matter has been dropped from the audit process, perhaps in a senior auditor's workpaper review. The internal auditor has a first responsibility to get resolution on the matter through the internal audit department up through the chief audit executive or the audit committee. If the internal auditor documents and reports the issue, but audit management elects to drop or ignore the matter, the internal auditor certainly then has the right and responsibility to report the matter through, hopefully, the enterprise's ethics hotline function or even through the SEC. Audit management and other processes should be in place to prevent such a frustrated internal auditor whistleblower situation.

Launching an Enterprise Ethics Hotline Function

Many enterprises today have established ethics hotline functions. Most include confidential telephone line facilities administered through the ethics department, human resources, or an independent provider. These toll-free telephone operations, which typically operate on a 24/7 basis, allow any employee or stakeholder to call anonymously and ask a question, report a concern, or "blow the whistle" on some matter. The idea is to provide an independent facility where all stakeholders can ask questions or report possible wrongdoing at any level. These are not legally required functions, but facilities where employees or other stakeholders in a larger enterprise can ask questions, report possible wrongdoing, or seek advice. The items reported may range from allegations of theft of company property, human resources complaints, or just to ask troubling questions. In most cases, the telephone operator will take all of the

necessary information, asking questions when needed, and then pass the reported incident to an appropriate authority for investigation and resolution. The hotline operator will typically assign the reported incident a case number, so the caller can later check on resolution.

Employee hotlines got established in many larger organizations beginning in the mid-1990s. Often knowledgeable human resources veterans, the operators are particularly skilled at answering human resources–related issues, such as treatment in the workplace. Where there have been allegations of wrongdoing, the recorded case is shifted to others for investigation, such as to the legal department. In some instances, these lines have turned into little more than corporate "snitch" lines where many minor gripes or infractions are reported, but they have generally been very successful.

While many established ethics hotlines were set up to be friendly in answering employee questions and giving some advice in addition to investigating reported incidents, using this same, already established facility for the SOx whistleblower program places some new controls and responsibilities on the function. While the more friendly help aspects of an ethics hotline can still apply, federal whistleblower rules require much more formalized processes, particularly in areas such as confidentiality, documentation requirements for all records, and efficient processing of any investigations. In addition, the employee calling in a SOx whistleblower allegation is legally protected from any future recrimination. In some respects, a bubble has to be encapsulated around the whistleblower employee such that there can be no actions of any sort directed at that whistleblower by the employer until the allegation is resolved. However, in order to establish an enterprise whistleblower reporting facility, control procedures need to be enhanced in any established ethics hotline facility. Exhibit 20.3 contains guidelines for setting up an ethics hotline program that will also serve as an enterprise whistleblower facility.

EXHIBIT 20.3 Guidelines for Setting Up a Whistleblower Call Center

- Establish independent—preferably toll-free—telephone lines and secure e-mail connections for the facility. The lines must not go through other company switchboards.
- Train all operators for the facility with the basic provisions of federal whistleblower rules. Also, establish scripts such that callers can ask the same general questions.
- Advertise and promote the facility throughout the enterprise with an emphasis that all items will be reported, the caller will be able to check status, all callers will be treated anonymously, and there will be no recrimination for caller actions.
- Implement a logging form to record all calls. Maintain the date and time of the call, the caller name or identification, and the details reported.
- Establish a routing and disposition process such that the status of who has the call information and the status of any investigation can be determined.
- Establish a secure database for all whistleblower data with appropriate password protection.
- Working with human resources, develop procedures to fully but anonymously protect any whistleblower from recrimination of any sort.
- Develop a process for closing out all whistleblower calls, documenting all actions, if any.

The existence of an ethics hotline and whistleblower facility will be of little value unless it is communicated and "sold" to all members of the enterprise. A good way to initially launch these processes is through the employee code of conduct discussed previously. Even if such a hotline has already been launched, the fact that the line can be used for any potential SOA whistleblowers needs to be communicated. The goal should be to investigate and promptly resolve all calls—and especially whistleblower calls—internally to avoid outside investigators and lawyers.

LAUNCHING AN ETHICS PROGRAM AND IMPROVING ENTERPRISE GOVERNANCE PRACTICES

A strong ethics program, based on a meaningful mission statement and a code of conduct, is a key element to any overall program of enterprise governance. The accounting scandals that led to SOx in the early years of this century were, in many respects, scandals at the top levels of the enterprise, whether caused by a scheming financial officer, a greedy CEO, or a don't-ask-any-questions public accounting firm. The executive teams at the accounting scandal companies set their own rules with little consideration given to the rest of the enterprise.

A strong ethics program will improve corporate governance practices for the entire enterprise rather than just the people in the executive office. The following five actions should be considered as part of launching an effective ethics and whistleblower strategy for the entire enterprise:

1. **Corporate policy.** An enterprise policy statement should be issued by senior management to emphasize that all stakeholders are encouraged, indeed have an obligation, to bring concerns about accounting and financial practices to the attention of management. The policy statement should also stress that management will not tolerate retaliation against employees who raise concerns. The policy can help foster an "open door" process for addressing issues, which, after all, is the most effective management approach.
2. **Employee concerns program.** A program must be established for the receipt and processing of concerns submitted by employees on a confidential or anonymous basis. An effective employee concerns program should include:
   - A central coordinator to process and investigate concerns.
   - Controls to ensure that an adequate investigation is consistently conducted, with proper documentation describing the resolution of the concerns.
   - A feedback mechanism to advise the employee of the disposition and resolution of the reported matter.
   - A process for periodically evaluating the effectiveness of the program.
3. **Training of supervisors.** Training should be conducted for all first-line supervisors and other managers on how to respond effectively to concerns raised by employees. Problems often escalate because of miscommunication between an employee and his or her supervisor. Cases of discrimination can turn on how a supervisor reacts to and handles a particular situation with an employee.

Thus there is a strong need for effective training of supervisors and managers on the subtleties associated with potential whistleblower concerns.

4. **Guidance to contractors.** Because public companies can potentially be on the hook for discriminatory acts by contractors, subcontractors, and other agents, special mechanisms should be put in place, such as specific employee protection clauses in contracts.
5. **Employee surveys.** Enterprises should periodically conduct surveys of their workforce to assess the corporate culture and gauge whether employees feel free to raise concerns.

Whether a major corporation or a small one, all are now subject to SOx rules and requirements. The ethics and whistleblower processes discussed in this chapter are important for SOx compliance and for good corporate governance.

NOTE

1. More information on Enron, WorldCom, and other corporations that precipitated the enactment of the Sarbanes-Oxley Act (SOx) can be found in many Internet sources and in Robert Moeller's book, *Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL* (Hoboken, NJ: John Wiley & Sons, 2008).

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER TWENTY ONE

Impact of Social Media Computing

NEW TYPES AND STYLES OF IT APPLICATIONS AND CONCEPTS have grown massively in recent years, with some significant new applications based on what are called *social media systems,* with names such as Facebook, Twitter, LinkedIn, and many others. These applications were originally directed at individual users, allowing them to post notes, pictures, and other friendly message materials over the Internet and among generally personal friends. Examples would be a teenager posting her picture and descriptions of a high school prom dance or proud parents posting photos and information on their new baby. These systems and messaging processes are generally known as social media computing applications, and many of their messages are very brief and sent via the texting functions available on many cellular phones. Social media systems are great tools for communication and certainly go beyond and for many are more popular than the Internet e-mail so common in today's business environment. Social network computing applications often can raise IT governance issues when used in enterprise business environments.

The objective of this chapter is not to provide detailed guidance on the use or technical aspects of these social computing systems or applications but to discuss IT governance issues when an enterprise that has freely allowed or even installed these systems is confronted with social computing governance and internal control issues. These systems are either officially or unofficially part of the IT infrastructure for many if not most enterprises today, and enterprise managers should take advantage of some of the positive benefits that can come from social media systems. They also should realize that social media IT systems and processes can present some IT governance risks to enterprises today.

WHAT IS SOCIAL MEDIA COMPUTING?

A social media application or system is an online service, platform, or IT site that focuses on building networks or relations among groups of people or users who share common interests and/or activities. Not too many years ago this was an unknown or undefined IT concept. Such a social media system has many more features and sometimes risks than the traditional e-mail system where each user on a network is identified by little more than an e-mail address with no further information about the subscriber. Rather, people with common interests or connections will log in to such a social media system through establishing their own automated calling card or a brief biographic profile describing the participant. Members of a network may post their photographs, biographical information, and descriptions of their activities, family, sometimes political opinions, or other materials. Virtually all social media services today are Web-based and allow users to interact over the Internet, through e-mail or instant text messaging facilities. Social media sites allow users to share ideas, activities, events, and interests within their individual networks.

Social media IT applications really got their start well before today's era of the all-pervasive Internet and even before laptop personal computers. The following are some of the major trends in the development of social media computing from their beginnings to the present:

- **1978 to 1989: One-to-few applications.** In the very early days of personal computers (e.g., Apple II or IBM PC), the first recognized social media application was called the Computerized Bulletin Board System (CBBS), created in February 1978 by Ward Christensen of IBM.[1] It was used by an IBM software development group to post messages about meeting times and locations, saving the time that had been spent in telephone calls. This was perhaps the first example where posted messages moved beyond one-to-one to a one-to-few type of interactive application.

  The Internet had not really been popularized at that time, and thousands of bulletin board systems, with names such as FidoNet, soon sprang up across North America and elsewhere, becoming useful and increasingly popular tools for communications between the geographically dispersed users who accessed these systems over telephone modems.
- **1990 to 1994: The growth of the Internet.** In the early 1990s, Internet usage was primarily available only to government, military, and academic organizations. This author, who was writing his first IT audit book at that time, had to find an acquaintance at a local university to give him written permission to establish an Internet account in order to access some IT audit-related documents. However, several commercial consumer-based Internet applications soon appeared with names like Prodigy and CompuServe. These services soon became what were called Internet service providers (ISPs) in major U.S. cities.

  Internet consumer acceptance soon received a major thrust from America Online (AOL), a company that aggressively marketed the Internet by sending out millions of AOL signup disks where participants could access the Internet and send e-mail messages, shop for goods, and participate in the new concept of online forums.

With the interactive opportunity to join online forums and broadcast e-mails, these applications were the first steps in scalable social media applications.

- **1995 to 1999: The dot-com bubble.** This era saw a major boom in Web technologies and Internet tools. Most of these new applications were based on new consumer products and merchandising; there was not much growth here in social media applications beyond the existing bulletin board sites.

  An exception from this era is SixDegrees.com, an early social networking Web site that lasted from 1997 to 2001 and was named after the "six degrees of separation" concept.[2] It allowed users to list friends, family members, and acquaintances on the site and allowed external contacts to join the site as well. Users could send messages and post bulletin board items to people in their first, second, and third degrees, and see their connection to any other user on the site. It was one of the first manifestations of a social networking Web site in the format now seen today.
- **2000 to 2004: The trend to social media grows.** Although all of the concerns about the year 2000 (Y2K) did not materialize into as big of a crisis as was predicted and the dot-com bubble began to recede, a series of new social media applications were launched during this period, including MySpace, Facebook, Friendster, LinkedIn, and others. We will be discussing some of these applications in greater detail in the sections following.

  Many of these new applications were widely used by people inside enterprise organizations and outside of the enterprise-controlled applications. Although there always had been some low-level chatter within enterprise systems, social media applications allowed people to create content and participate in discussions without organization participation—an almost subversive trend!

  Another Internet platform application launched during this period, WordPress, allowed individuals with no programming knowledge to build and launch blog sites, personal diaries, or content sites. Using such a tool, a person could host a blog on his or her own domain site and have essentially full control over its design and contents. This was a major move to personal journalism.
- **2005 to 2009: Social networking applications continue to grow.** Social media applications have continued to grow and evolve, with applications such as YouTube, a video-sharing Web site where anyone can become a publisher of video content. Smartphones have become very popular, to which a user can download a wide variety of applications. Perhaps the most significant new social media application during this era was the launch of Twitter, a microblogging application where a user can publish short content-based messages and follow others through short bursts of information. We will introduce Twitter further in a section following.
- **2010 and beyond:** Our use of social media applications continues to grow, causing many IT governance issues and concerns in today's enterprises. For example, world events during the first months of 2011 included what was popularly known as the Arab Spring, where autocratic political leaders in Tunisia, Egypt, and Libya were brought down. In each of these cases, the antigovernment protests were initiated after massive social media chatter over Facebook and other such vehicles. People saw events that enraged them and posted their comments and photos to others, who passed them to still others. The results were surges of popular protests that soon toppled these governments.

While people using the likes of Facebook to topple an autocratic government is a strong example of the power social media, these same tools have and continue to present challenges to business enterprises today. Social media tools or services can present IT governance challenges to enterprises. For many today, these systems are almost too new, and enterprises with traditionally controlled IT systems and applications often are not in a position to easily adapt to the open, flexible nature of social media systems. Also, individual members of an enterprise often will be individual users of their own social media computing application. This can present IT governance problems if an enterprise has not established appropriate rules and procedures covering its social media operations.

SOCIAL MEDIA EXAMPLES

The sections following discuss three very popular but each quite different social media applications—Facebook, LinkedIn, and Twitter—as well as some of the unique governance issues surrounding each of these applications. Each started as a personal application, but people have moved them into the workplace through their workplace communications on individual laptop systems or smartphones.

Facebook

Facebook is a social media service and Web site that was launched in February 2004 by Mark Zuckerberg along with several of his college roommates at Harvard as a means to communicate and share information among fellow students. Originally limited to just Harvard students, Facebook was quickly expanded to other colleges in the Boston area, the Ivy League, and then Stanford University. Growing by word of mouth, it gradually added support for students at other universities before then opening to high school students and others. Today, Facebook has become a very popular system used by many, many people worldwide. In addition, for many today it has replaced e-mail as a means of communication among individuals.

From its limited college dormitory start in 2004, as of August 2012, Facebook had more than 950 million active users, with the number of users continually growing. Starting as a private company, Facebook has recently gone public.

Facebook individual users often first get started by someone, usually a personal friend, sending them an e-mail message and asking them to become their Facebook "friend." The new user will then be asked to create a personal profile, add other users as friends, and exchange messages, including automatic notifications when they update their profile. Additionally, users may join common-interest user groups, organized by workplace, school or college, or other characteristics.

Joining Facebook

For many senior-level business professionals, Facebook is more than just an IT application. It is almost a concept, which a senior business professional may have read about, even though that same senior executive often has no understanding of the system

beyond the comments and Facebook activities of his or her usually IT-savvy children. This is particularly true if one has college-age or high-school-age children who understand and use Facebook. Of its millions of users, some 60 percent of Facebook users are under the age of 35.

One often becomes first involved with Facebook through receiving an e-mail from a business associate or relative asking that recipient to become a "friend" of that person on Facebook. Exhibit 21.1 outlines the steps to log into Facebook. The idea is that one logs in based on the initial invitation and then can connect with others who also are Facebook users. Facebook friends can connect with others in a cascading manner such that friends of friends can be connected to create an expanding network.

Using Facebook

Much more than just an alternative way to use an e-mail system, Facebook allows you to build up a profile about yourself, to post messages to everyone on your friends list describing your activities, to share a message with your Facebook friends, and much more. These messages, both text and pictures, can be either e-mail-like notes or brief text messages through a mobile smartphone. Of course, in its college dormitory environment, those posted messages were often descriptions and pictures from a recent party or some other event. They typically are just a posted note and do not require or solicit a response. A Facebook user can send a specific note or post a question to anyone or all persons on the user's friends list. Those messages may then be forwarded to still others.

EXHIBIT 21.1 Steps to Joining Facebook

Step 1.	Visit the Facebook Web site (www.facebook.com).
Step 2.	Fill in your full name, a valid e-mail address, and birth date. In addition, one should enter as much personal information as one wishes to broadcast in the Facebook "About" section. This might include work address, educational background, and any of many other areas of personal interest. One could also include a digital photo, a picture of one's spouse and family, and other personal information here. The new Facebook user can also select "None of the above" here to be just a name with little personal information.
Step 3.	Choose your password. Enter an easy password to remember of at least six characters.
Step 4.	Complete the image verification check. Identify the words or numbers displayed and type them in.
Step 5.	Read the Facebook Terms of Use and Privacy Policy. Check the box to mark your agreement with the terms of both.
Step 6.	Click on the "Sign Up!" button at the bottom of the page and wait for redirection to a thank-you page.
Step 7.	Check your e-mail inbox and click on the confirmation page from Facebook. It will send link confirmation for your registration.

Facebook postings can give someone a detailed description of one's personal life and activities, depending upon the level of privacy selected. For example, after logging into Facebook, one can enter in the name of an acquaintance who may be registered in Facebook—or anyone for that matter—and look at that person's posted profile, recent Facebook postings from others, and gain access to that person's Facebook friends, even looking at their postings as well. We will talk more about business privacy concerns here in a section following, but if a Facebook user has not designated his activity as private, one can sometimes find out more about a person than they would want to. For example, one can see "Thank you for inviting me to . . ." types of messages that have been sent to a person, sometimes with a photo, as well as the ability to go to that sender's Facebook page. These messages remain posted for an extended period, unless deliberate steps are taken to delete records. While this is all great for college student life, the postings and recorded activities could cause privacy and even security concerns in a business environment.

The Facebook concept also can also be useful in a business environment as means to build and manage workforce teams. For example, for a large systems implementation project—along the lines of an effort described in Chapter 16 on project and program management—the project administrator can ask all project team members to create or update their Facebook profiles to establish them as members of the project team. Project events can be easily scheduled and communicated, and the manager interested in the backgrounds of team members can access their profiles in a friendlier manner than the typical human resources records.

Our description highlights only a few of the ever-expanding Facebook features. One can subscribe to download postings from selected Web sites, post messages or communicate through a smartphone, and receive a birthday message that is posted to all of one's Facebook friends. For a business enterprise, Facebook can present risks. For example, an employee can complain in a Facebook post about the quality of some company product or even the competence of a manager. What was intended as a personal message to a Facebook friend can be picked up by that friend and then sent to friends of friends to establish widespread and sometimes damaging nets of communications about the enterprise or specific issues. As will be discussed in the section following on social media legal issues, there are multiple IT governance issues here.

Although Facebook has a component for building enterprise business pages that is a powerful tool for marketing all aspects of an enterprise's business operations and there is a current surge in the use of Facebook as a business communications tool, its typical use today is not for business but for personal communications. Creating a Facebook business page is a good method of promotion because Facebook business pages are viewable by millions of Facebook users. These Facebook pages are an effective advertising platform offering innovative methods of Web marketing, allowing for interaction among business owners and customers. They really go beyond the IT governance issues theme of this chapter as they represent a strong and powerful enterprise application.

LinkedIn

LinkedIn is a popular social media application based around business-related social or professional networking and used for networking-type communications among

multiple professional groups, such as members of the AICPA or college alumni groups. LinkedIn is also a popular communication platform for many professional groups such as project managers, civil engineers, geologists, auditors, and many others. It operates worldwide and in multiple languages. At the time of publication, there were over 125 million LinkedIn registered users.

Most professionals first encounter LinkedIn through an e-mail from a professional associate with an invitation to join some LinkedIn group or establish a LinkedIn connection of common professional interest. If new to LinkedIn, that invitee is asked to register by posting some personal information and often a professional résumé. This is a bit more formal than Facebook, where one is simply asked to become someone's Facebook "friend" almost without the need of an application.

When registering with LinkedIn as part of a professional group, the user is asked to provide professional résumé-type information, current and past employers as well as the dates of those jobs, and other personal professional information. There is also space to post a full résumé, advertisements, and other materials. The system also has a process where the new registrant can request past employers and professional contacts to provide references.

LinkedIn allows registered users to maintain a list of contact details of people with whom they have some level of relationship, called *connections.* Users can invite anyone (whether a site user or not) to become a connection, but the recipient of an invitation can select "I don't know" to reject the person's invitation. LinkedIn connections can be used in the following ways:

- A contact network can be built up consisting of someone's direct connections, the primary connections termed *second-degree connections*, and also the connections of second-degree connections termed *third-degree connections.* This can be used to gain an introduction to someone a person wishes to know through a mutual contact.
- LinkedIn can then be used to find jobs, people, and business opportunities recommended by someone in one's contact network.
- Employers can list jobs and search for potential candidates.
- Job seekers can review the profile of hiring managers and discover which of their existing contacts can introduce them.
- Users can post their own photos and view photos of others to aid in identification.
- Users can follow different companies and get notifications about the new products or other information.
- LinkedIn's "gated-access approach" requires contacts among professionals to have either a preexisting relationship or the intervention of a contact of theirs and is intended to build trust among the service's users.

Within its various specialized topic areas, LinkedIn sites are active discussion forums covering LinkedIn specialty areas. For example, a LinkedIn site for the National Association of Corporate Controllers[3] has a series of active discussions. A LinkedIn member of that group may pose a question such as, "How should the board better manage its internal auditors?" Others then may enter a response, and the result may be a heated back-and-forth ongoing discussion.

Perhaps more importantly than its professional contacts features, LinkedIn includes a series of specialized applications with objectives to get job leads, analyze business traffic, promote product sales, promote brand awareness, handle ticket sales, communicate with investors, and more. The LinkedIn Polls application is a good example. It allows LinkedIn users to easily find answers to business and market research questions. It allows an enterprise to ask some question and LinkedIn will distribute it to your connections and millions of other professionals on the site. The poll results can be shared with enterprise Facebook or Twitter integrations, or embedded in an enterprise's Web site. It operates just like any other polling service: LinkedIn users can ask a question, add up to five potential responses, and choose how long it will run. Once responses have been received within the specified time period, LinkedIn shares the responses with established social networks or enterprise Web sites. Because of this LinkedIn link, poll responses can be broken down voting by age, gender, or seniority, allowing management to analyze such questions as, "Do 25-year-olds answer differently from 45-year-olds?" or "Do men and women answer differently?"

LinkedIn is more of a business application and does not have the same open-environment potential exposure risks that can be found in Facebook, where messages to Facebook friends are easily circulated and recirculated to others. However, because it is a professional communication and discussion vehicle among various professional specialized groups, confidential enterprise data can easily slip through LinkedIn discussion sites. A product development engineer, for example, may have subscribed to a LinkedIn site for enterprise product development engineers. As part of LinkedIn's ongoing online discussions, that development engineer might inappropriately respond to an online discussion by giving some enterprise confidential information to make a technical point but not realizing the nature of the data released. In addition, that engineer's résumé may be open to outside recruiters, a potential drain on company resources.

Twitter

Many in the United States first heard about Twitter in 2011 when a then–U.S. congressman, Anthony Weiner, tried to send a lewd photograph of himself on Twitter to a female campaign staff aide but mistakenly sent the photo to his Twitter distribution list (*followers* in Twitter lingo).[4] The press soon reported that the then-congressman was sending out many other such racy Twitter messages. These actions forced Weiner to resign, and his shenanigans certainly caused many to hear about the potential power of Twitter.

Twitter is a free service that allows anyone to say almost anything to anyone as long as it is in 140 characters or less—it is a "what are you doing right now" type of system that permeates online social communication. Based around its bluebird logo, Twitter enables its users to send and read these short text-based posts or brief messages, informally known as "tweets," often through a mobile phone, either by text messaging or by apps released for certain smartphones. With all of this message traffic, Twitter is one of the ten most visited Web sites worldwide. A February 2009 survey by Compete.com references Twitter as the third most used social network based on their count of 6 million unique monthly visitors and 55 million monthly visits. To help explain Twitter's terminology and concepts, Exhibit 21.2 lists a few Twitter terms and concepts. More senior managers may find their staff members using these terms as they tweet messages to others.

EXHIBIT 21.2 Twitter Terms and Concepts

- **Tweet.** When you post or write your 140 characters on Twitter and hit send it's a tweet or tweeting.
- **Handle.** The term for a user's Twitter name in the format @ducttape; a short personal name similar to a URL.
- **Follow.** This is the act of adding someone to your list of the people you are following, making their tweets show up on your home page.
- **Replies.** This is when someone writes a tweet directly at a user's handle—@ducttape cool post today blah blah—and is also often an invite to engage with another follower.
- **Retweet.** This is a tactic of republishing someone else's tweet—the original tweet along with the author's handle stays intact, but you are basically showing someone's tweet to your followers—Many use this to add content and acknowledge the materials from the people they follow.
- **DM.** This is the term for a message that is sent directly to another user. That person must be following you in order for you to DM him or her. This is a very useful tool for private messages.
- **Hashtag.** This is a way people categorize tweets so that others might use the same tag and effectively create a way for people to view related tweets.

With Twitter's ability to track and carry a wide range of messages about a wide variety of people and subjects, a Twitter user and sometimes an employee may be spending too much time reading and sending these tweets. For example, San Antonio, Texas–based market research firm Pear Analytics analyzed 2,000 tweets (originating from the United States and in English) over a two-week period in August 2009 and separated the messages into six categories:[5]

1. Pointless babble—40 percent
2. Conversational—38 percent
3. Pass-along value—9 percent
4. Self-promotion—6 percent
5. Spam—4 percent
6. News—4 percent

These results indicate that Twitter often contains too much "pointless babble," the first item on the above list. Perhaps the advantage here is that these messages allow Twitter correspondents to know what the people around them are thinking and doing and feeling. However, a lot of this activity is similar to company staff talk sessions around the company watercooler from a past era. The astute manger back then frowned on or limited such watercooler chat activity. Attempts should be made to treat staff social media workday usage in the same manner.

Whether it be the example of the rogue ex-congressman Weiner, discussed previously, or any of many other current examples, Twitter is a powerful tool that can present risks to an enterprise if used inappropriately. Just as we discussed the importance of enterprise codes of conduct in Chapter 20 and the need to determine that all impacted stakeholders have read, understand, and agree to comply with that code of

conduct, an enterprise should launch a similar policy for social medial applications such as Twitter.

Exhibit 21.3 is an example enterprise policy for employee use of Twitter using our Global Computer Products sample company. Similar policies could be implemented for Facebook and others, or the policy could be structured in a manner that includes enterprise social media applications. The key is that any such policy must be launched in a manner such that all employees and other stakeholders understand its purposes and the potential risks of any such social media applications.

EXHIBIT 21.3 Sample Policy for the Use of Twitter

Employee Policies
Global Computer Products

Employee Corporate Policy – xxx

Policy for the use of Twitter

Purpose. This document describes the use of personal Twitter accounts during an employee's workday. It does not apply to corporate Twitter accounts.

Overview. The company realizes that employee social networks and social media tools provide some value to the company. As a result, we have established a policy that allows for a small amount of usage of Twitter while at work as long as certain guidelines are met. If the guidelines laid out in this policy are deemed unacceptable, then an employee's use of Twitter while at work is also deemed unacceptable.

This document provides two sets of guidelines. The first set is applicable to all Twitter usage for company-related activities, whether at work or on personal time. The second set is applicable to those who wish to use Twitter at work and use their accounts to help promote the company.

Guidelines for Twitter Use at Global Computer Products

1. Do not disclose confidential or proprietary information on your Twitter account. Disclosing competitive information or trade secrets is cause for termination.
2. Be responsible for what you write. Remember that just because you "can" say something doesn't mean that you should. Written words are more difficult to interpret than verbal interaction. Remember that what you say will be a permanent record. Be careful. Be smart.
3. Be authentic and use full disclosure. If you are discussing a company product or that of a competitor, it is in your best interest to disclose that you work for the company.
4. Respect copyrights. Don't post text, images, or video that were created by someone else without proper attribution. If you have questions about copyright law and/or usage of certain media, contact the legal department.
5. Twitter is not a substitute for intra-company communications. Important information should be transmitted within normal company communication channels, not on Twitter.

(*Continued*)

EXHIBIT 21.3 (*Continued*)

6. Twitter is not a substitute for customer service. Please refer customers to the customer service department instead of handling inquiries entirely through Twitter.
7. Be clear that you are not an official spokesperson for the company and that your views do not necessarily reflect those of the company.

Guidelines for Twitter Use at Work

1. You are required to provide either (a) a link to the company website or (b) a company logo on your Twitter page.
2. You are required to perform an @company Twitter transaction at least once a week.
3. Some portion of your tweets should be related to the company and/or the industry in which we operate. There is no specific numeric requirement you must meet, but 20% of total tweets is deemed an ideal level.
4. Remember to be productive. Twitter can be a time sink and can prevent you from completing other work-related tasks. Use good judgment to insure that you have plenty of time to complete all of your regular work.

I have read this Global Computer Products policy regarding my use of Twitter, I understand this policy guidance, and I agree to abide by the rules and guidance outlined in this policy.

Name:_____. **Employee Number:**_____.

Signed:_____. **Date:**_____.

ENTERPRISE SOCIAL MEDIA COMPUTING RISKS AND VULNERABILITIES

A valid senior executive question might be, "I am an enterprise senior manager. Why should I be concerned about our employees and other stakeholders using Facebook, Twitter, and other social media tools in the business work environment as long as they are doing their jobs?" That is the type of question that many senior managers ask when they do not really understand these ostensibly friendly and personal applications.

Social media sites often seem friendly and exist outside of the radar screen of many business systems, processes, and concerns. They are too often viewed as an employee diversion, like the joint efforts of a planning committee for the annual holiday party. However, social media issues can go beyond just friendly social messages, as other people can see this message traffic and potentially initiate actions based on the communications.

A recent *Chicago Tribune* article highlighted how employee Facebook chatter can cause trouble to an enterprise. The staff members at an auto dealer talked flippantly

among themselves over Facebook about how their employer was probably ignoring U.S. labor laws.[6] Their supposedly private messages were eventually passed on to U.S. labor law authorities, with resultant legal actions against the employer. Messages sent through social media systems present some risks!

Sometimes social media systems are viewed as almost an HR-related resource, like an unofficial company newsletter. However, an enterprise faces many risks in social media systems, including loss of reputation and possible liability when employees blab or post photos and videos about what they shouldn't. There are also the computer security risks of malware, identity theft, what is called *phishing,* and the privacy breach of sensitive data that was introduced in Chapter 10.

The risks associated with employee use of Facebook, Twitter, and other social media should really be considered beyond the IT security department, as the primary responsibility of enterprise management. These applications are generally operated over the Internet and outside enterprise-controlled systems.

Many of the IT social media risks and management concerns are tied to the individual behavior that takes place outside the infrastructure boundaries of the enterprise and its IT systems. However, social media systems carry with them issues related to content and freedom of speech. These social media practices are very much tied to many of the issues in the discussion on the need for an ethical workplace culture in Chapter 20. That chapter discusses the importance of strong management messages and policies such as codes of conduct and mission statements to help get an enterprise and its stakeholders thinking in a correct and positive manner. However, an enterprise should be aware of some of the following social media risks and concerns:

- **Employee productivity issues.** It is perhaps more of a management issue in terms of setting employee goals and responsibilities, but employees at all levels can sometimes spend excessive amounts of time sending notes and pictures to friends, both inside and outside of the company, whether over Twitter, Facebook, or some other social media application. In some respects, this is not too different than people spending excessive amounts of time on personal telephone calls, but this social media activity is sometimes hard to detect and monitor.
- **Lack of control over corporate content.** Employees and stakeholders may innocently or deliberately post wrong or improper information on social media sites. This type of information can be passed on to many others through the cascading nature of many social media tools. Once the false information has started to spread, it is difficult to stop.
- **Noncompliance with record management regulations.** Despite copyright and data protection rules, it is very easy for stakeholders to copy and communicate protected documents over social media systems. An enterprise faces risks if such records are improperly or illegally communicated.
- **Viruses and spyware.** There have been reported incidents where social media or related networking sites have been used to spread malware such as viruses,[7] and social media systems are certainly not unique here. Realistically, however, social networking sites probably pose no more of a threat than any other type of Web site.

- **Bandwidth problems.** Much more of an issue in the earlier days of telecommunications and the Internet, bandwidth refers to the "size of the pipe" or the amount of data transmitted over communications lines. People sending large volumes of digital photographs or other high-volume material can somewhat choke a system. While this is not too great of an issue over the Internet, such high-volume materials can all but clog a communications line for a smaller enterprise.
- **Enterprise security issues.** There is much vulnerability here. A perpetrator, for example, can use a cell phone to take a picture of a confidential document, product, or facility and then easily transmit that material to one or many over a tool such as Facebook with just a few quick keystrokes. Physical controls, well-communicated policy statements, and a strong enterprise ethical environment are needed.
- **Social media liability issues.** An enterprise could be held liable for postings by an employee made on company time through enterprise IT resources. While the law really is not clear at this point in time, individuals have been found liable for incautious postings to social networking sites. An enterprise should exercise caution here, and it is possible that businesses could, too. It is a risk you should certainly consider.

As our use of social media tools grows, we can only expect this trend to continue. Because most enterprise stakeholders have their own smartphone device as well as a home system with Internet connections, virtually all of these people have access to social media sites. Some make extensive use of these tools, and the boundary between personal activities and office systems can quickly become fuzzy. An enterprise is looking through rose-colored glasses if it tries to implement a workplace policy of no social media IT activities while on the job. We generally are not working at a facility on a nine-to-five basis but are involved in work activities in the home office or while traveling as well. We cannot draw lines here.

Social media tools are also growing in the workplace. Our earlier discussion of LinkedIn discussed its polling tool, which can be a common and frequently used social media application in the workplace. We will increasingly be seeing the lines between social media applications for primarily personal purposes and the use of these applications as business tools becoming more closely linked. The only way to limit risks and to have a better IT governance understanding of the use of social medial tools in the workplace is to establish and effectively communicate policies about the effective use of these tools to all stakeholders in the enterprise workplace.

SOCIAL MEDIA POLICIES

An enterprise needs to establish educational practices, outlining the dos and don'ts for various social medial media systems as well as some very specific policies covering the stakeholder use of these tools. These social media policies should be almost a subset of corporate policies such as codes of conduct as well as IT security and privacy policies that are communicated to all employees and stakeholders. For example and discussed in greater detail in Chapter 20, an enterprise should develop an overall stakeholder-specific social media policy that outlines company policies in a very high-level but easy-to-understand manner. The code should be refreshed and updated regularly and all

stakeholders should be asked to periodically affirm that they have read the code, understand it, and agree to abide by it. Implementing such a code of conduct is important for strong and effective enterprise IT governance practices. Exhibit 21.4 is an example of a general enterprise social media policy that would be designed to apply to all stakeholders using enterprise social media applications, ranging from staff members to senior management, and applicable to all social media applications that have an impact on the enterprise, whether an enterprise-based initiative and an application based on the system at home or a personal device.

EXHIBIT 21.4 Enterprise Social Media Policy

This policy applies to all social media tools, used both on and off the job, for enterprise business operations. Beyond the more specific guidance discussed below, anyone using social media tools on either personal or enterprise business should:

- Treat others as you would like to be treated.
- Add value to your consumers, your industry, and your business.
- Be respectful, professional, and courteous.
- Provide insight, expertise, and relevant conversation.
- Communicate ethically and morally in support of your professional goals.

In addition, all enterprise stakeholders should keep the following principles in mind:

Think before you post

Keep in mind that most online social computing platforms are like public marketplaces—what's out there is available for all to see. On social platforms, the boundaries of professional and personal information are not always very clear. In these days of shifting privacy policies and powerful search engine indexing, you can't always be sure what is being shared, viewed, or archived. Note that what you publish online will be public for a very long time. What you post will reflect on you, so be consistent with the way you would wish to portray yourself to the company, friends, family, colleagues, and clients.

If you are unsure whether certain content is appropriate to share online, then don't post it. It's better to be safe than sorry.

Responsibility

You are personally responsible for your words and actions, no matter where you are, even in the online world. Please remember that when you participate in social media, you are speaking as an individual and not on behalf of the company. Always identify yourself using the first-person singular.

When you discuss company-related information online, be transparent by giving your name and role and mentioning that you work for the company. If you have an individual site that refers to or has an impact on the company, use a disclaimer such as "The views expressed on this site are my own and not those of [*company name*]."

Where applicable law permits, know that the company reserves the right to monitor use of social platforms and take appropriate action to protect against misuse that may be harmful to the company's reputation.

Establishing a company account or becoming an official representative who shares information about the company and the areas we work in requires approval from appropriate levels of management. Only these accounts may display the company logo.

(*Continued*)

EXHIBIT 21.4 (*Continued*)

Conduct

Your behavior online should be consistent with our Code of Business Ethics.

You have the opportunity to help shape the company's reputation online. Use your expert knowledge to enrich discussions, help solve problems, share the excitement of our work environment, and promote learning and idea-sharing.

Always remember that the tone you use online can be interpreted in different ways by your readers, due to a lack of nonverbal communication or cultural differences. Some participants may not be familiar with abbreviations, emoticons, and other common codes used in online communication. Remember also that comments are often taken out of context, so stick to the facts.

Trust is the key element in building relationships online. Build trust by keeping a respectful tone, even when disagreeing with others, and by responding to comments in a timely manner. If you realize that you've make a mistake, try to correct it promptly.

Do not engage in any conduct online that would not be acceptable in your workplace or that is unlawful. For example, do not make derogatory remarks, bully, intimidate, harass other users, use insults, or post content that is hateful, slanderous, threatening, discriminating or pornographic.

Confidentiality

Always protect our companies', clients', and suppliers' confidential and other proprietary information. Don't put anything online you wouldn't share with a journalist, client, analyst, or competitor.

Make sure any reference to business information, customers, and suppliers does not violate any nondisclosure obligations. Please also remember your confidentiality obligations under your employment agreement.

Don't disclose information about colleagues or other persons, misuse their personal data, or publish their photos without their permission.

Always use good judgment regarding information that could be of a sensitive nature. Don't use social computing platforms to exchange information that is company, customer, or supplier confidential, unless access has been cleared for receipt of such information and the platform has been cleared for appropriate security levels. Public sites are not appropriate sites for internal communication with other company employees.

Copyrights

Comply with laws and regulations and more particularly with laws governing intellectual property rights, including copyrights and trademarks.
You must not post content or take any action that violates the law or infringes company or any third party's intellectual property rights.

Final thoughts

Use of social computing platforms in accordance with this policy can be a very effective and powerful communication tool. Be proud of what you do and enjoy a sense of accomplishment in the search for better quality and greater efficiency. Above all, please use good judgment, be attentive to others, and take the trouble to listen and be understood.

Depending on the level of use in the enterprise, comparable policies can be launched for Facebook and other social media applications. While a general policy can be drafted for all social media applications for an enterprise, it is usually best to develop specific policy statements for each application, such as Twitter and Facebook. The idea is to get the message to all stakeholders that their use of various social media applications in the workplace carries some risks as well as opportunities for the enterprise and their career paths.

Social media applications present some strong IT governance issues for today's enterprise. While the Facebook, Twitter, and LinkedIn applications that have been briefly introduced in this chapter are perhaps the most common today, this is no guarantee that they will be as prominent a few years hence. However, their concepts represent a sea change regarding the manner that information is developed and processed that almost certainly will not change. Although senior managers may look on these applications as tools for their children at home or at school, as well as younger associates on staff, every senior manager should at least become hands-on familiar with these tools in order to better understand them and communicate with others in the enterprise.

NOTES

1. Scott Gilbertson, "Feb. 16, 1978: Bulletin Board Goes Electronic," *Wired*, February 16, 2010, wired.com/thisdayintech/2010/02/0216cbbs-first-bbs-bulletin-board/.
2. Six degrees of separation refers to the idea that everyone is on average approximately six steps away, by way of introduction, from any other person on earth, so that a chain of "a friend of a friend" statements can be made, on average, to connect any two people in six steps or fewer.
3. An executive can join the National Association of Corporate Controllers (NACD) site by logging into LinkedIn and then clicking to join the NACD group. That site's administrator will review the requester's credentials and potentially accept them and then later allow them to participate in NACD discussions.
4. "Anthony Weiner Resigns: Timeline of Photos, Twitter Scandal Fallout," *Huffington Post*, June 16, 2011, www.huffingtonpost.com/2011/06/16/anthony-weiner-resigns-scandal_n_878161.html; "Rep. Anthony Weiner Retains Lawyer amid Frenzy over Lewd Twitter Photo," Fox News, May 31, 2011, www.foxnews.com/politics/2011/05/31/rep-weiner-retains-lawyer-amid-frenzy-lewd-photo/.
5. Jennifer Van Grove, "Twitter Analysis: 40% of Tweets Are Pointless Babble," Mashable Social Media, August 12, 2009, http://mashable.com/2009/08/12/twitter-analysis/.
6. "Social Media Emerges as Battleground for Protected Speech at Work," *Chicago Tribune*, September 2, 2011, http://articles.chicagotribune.com/2011-09-02/business/ct-biz-0902-chicago-law-20110902_1_social-media-labor-laws-employment-law.
7. A Google search will show numerous reported incidents here. For a sample commentary, see "Should Social Networks Be Banned at the Workplace?," SocialSmarty, http://socialsmarty.com/small-business/should-social-networks-be-banned-at-the-workplace/.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

CHAPTER TWENTY TWO

IT Governance and the Audit Committee's IT Role

THE PREVIOUS CHAPTERS HAVE DISCUSSED many aspects and processes to understand and improve enterprise IT governance. Our IT governance comments and suggested actions have been directed to all types and sizes of business enterprises, although we have been more focused on the larger, multinational corporation, with multiple units often spanning international boundaries. Some of these IT governance practices also can be costly for the smaller enterprise, while others require significant management contributions. When implementing any IT governance process, management should always consider the costs involved and then balance them against the benefits received.

This last chapter concludes with a discussion on the role of the board of directors' audit committee, an extremely important element in corporate and IT governance. We too often think of the audit committee only in terms of its role in supervising the internal audit functions as well as coordinating external audit activities. The audit committee also sets the tone for many IT governance activities. This chapter will briefly review the audit committee's role in establishing the tone for and reviewing enterprise IT governance activities.

THE ENTERPRISE AUDIT COMMITTEE AND IT GOVERNANCE

Public corporations are managed by boards of directors, elected by shareholders, and responsible for major management activities. Elected board members may sometimes be members of management or may be independent directors with no other direct corporate ties. An audit committee is a key component of a corporate board of directors, with responsibility for internal controls and financial reporting oversight. Because of this oversight responsibility and Sarbanes-Oxley (SOx) requirements, audit committee

members must be independent directors with no connection to enterprise management. There are no size restrictions, but a full board with 12 to 16 members often has a 5- or 6-member audit committee. An audit committee may invite members of management or others to attend committee meetings and even to join in on the committee's deliberations. However, outside guests cannot be full voting members, per SOx rules. An enterprise's board of directors is a formal entity given the responsibility for the overall governance of that enterprise for its owners, investors, or lenders. All members of the board can be held legally liable through their actions on any issue, and a board and its committees enact most formal business through resolutions, which become matters of enterprise record.

As a clarification here, corporate boards may consist of what are known as inside or outside directors. Inside directors are regular members of management who are also serving on the board of directors. For example, CEOs and CFOs sometimes have dual roles of managing their executive job functions and then overseeing those same operations by serving on the board. As senior executives in the enterprise, inside directors should have extensive knowledge about their corporation but may not always act in the interests of outside, independent shareholders and investors. This has led to criticisms that inside directors are sometimes the foxes guarding the chicken coops.

An outside director, or what is more frequently called an independent director, is someone who does not have any direct affiliation with day-to-day corporate operations and does not draw a salary from the corporation, besides directors' meeting fees. Independent directors typically fly into town for board meetings and do not have permanent offices or staffs in an enterprise. They are considered to be in a better position to make such decisions as the closing of an office, as they will not be perceived as having any personal interests.

In the years prior to Sarbanes-Oxley, many corporations had boards of directors consisting of company officers and friends and associates of the CFO. The latter group were sometimes quite unqualified for those board positions and acted at the CFO's bidding. Things really came to a head with the fall of Enron and the launch of the Sarbanes-Oxley Act in around 2002–2003. The U.S. congressional committee investigating the Enron debacle found, among other matters, a not very independent board, which benefited from "consulting contracts" awarded to it by the CFO as well as having a demonstrated lack of personal understanding of Enron's complex financial transactions at that time.

The SOx legislation, as discussed in Chapter 2, mandated a series of board of directors' requirements with objectives of improving corporate governance. Among them, an audit committee must now consist only of outside directors—giving it independence from management—and is, or at least should be, composed of a specially qualified group of outside directors who understand, monitor, coordinate, and assess the internal controls environment and related financial activities for the entire board. In order to fulfill its responsibilities to the board of directors, stockholders, and the public, an audit committee needs to launch and manage an internal audit function that should become an independent set of eyes and ears inside the enterprise, providing assessments of internal controls and other matters.

These comments are based on a corporate structure such as one with stock registered with the Securities and Exchange Commission (SEC), but other nonpublic

enterprises also can benefit from this audit committee structure. For example, many not-for-profit or private enterprises are large enough to have a formal board of directors and an internal audit function. Although it is not mandated by SOx and SEC rules, these organizations will also benefit from a board audit committee consisting only of independent directors.

The audit committee has an overall responsibility for an enterprise's external and internal audit functions. External auditors have a prime responsibility to an enterprise's board of directors for attesting to the accuracy and fairness of the financial statements. While external auditors are independent, the audit committee reviews and approves external audit budgets, receives reports from them, and will have ongoing communications with the partner in charge of the audit engagement. Although an external audit firm may serve an enterprise over many years, the audit committee has the right to change external auditors if there have been disputes over services, budgets, or other matters.

The audit committee is responsible for internal audit and its IT auditors, who have a large role in assessing internal controls over the reliability of financial reporting and IT processes, the effectiveness and efficiency of operations, and the enterprise's compliance with applicable laws and regulations. In particular, internal auditors and their IT audit specialists assess the many IT-related security and integrity risks and IT governance issues facing an enterprise.

Internal audit functions are governed through an audit committee–approved charter defining their activities and relationship with the enterprise's audit committee. These charters typically require the audit committee to:

- Review the resources, plans, activities, staffing, and organizational structure of enterprise internal audit. Regarding IT governance activities, these areas are summarized in Chapter 19.
- Review the appointment, performance, and replacement of the chief audit executive (CAE), the officer responsible for internal audit.
- Review all audits and reports prepared by internal audit together with management's response.
- Review with management, the CAE, and the independent accountants the adequacy of financial reporting and internal control systems. This includes the scope and results of the internal audit program, and the cooperation afforded or limitations, if any, imposed by management on the conduct of the internal audit program.

These requirements have been part of the relationship between internal audit and its audit committee over time. The CAE should work closely with the audit committees to ensure that effective communication links are in place. The third point mentioned on audit reports is an example. Prior to SOx rules, some internal audit functions supplied their audit committees only with summaries of internal audit report findings, or even submitted reports on what the CAE decided were "significant" internal audit report findings. With today's SOx rules, internal audit provides the audit committee with all audit reports and their supporting management responses, including sometimes fairly technical IT audit reports that internal audit management keeps from audit committee reviewers.

An audit committee usually is not involved in day-to-day administrative matters regarding the internal audit function and its CAE but must ensure the ongoing quality of the internal audit function. For example, the audit committee should carefully review annual audit plans and ask appropriate questions regarding the findings and recommendations from internal audit reports. In addition, the audit committee has the ability to hire or fire the CAE, but there should be an ongoing level of cooperation here. The audit committee is not on-site on a daily basis to provide detailed internal audit supervision and must rely on enterprise senior management for some detailed support.

The CAE or the internal auditors cannot just ignore appropriate management requests by claiming they report only to the audit committee and are not responsible to enterprise line management. Similarly, enterprise management must make certain that internal audit is part of the enterprise and not an outsider because of the audit committee relationship.

AUDIT COMMITTEE IT GOVERNANCE RESPONSIBILITIES

The audit committee should develop an overall understanding of the total audit needs of the enterprise. This high-level appraisal covers various special control and financial reporting issues, allowing the audit committee to determine the portion of audit or risk assessment needs to be performed by either the internal or other audit providers. As part of this role as the ultimate coordinator of the total audit effort, the audit committee is responsible for reviewing and approving higher-level plans and budgets of internal audit. Although enterprise management may have its own ideas about the total audit effort and how it should be carried out, and although the CAE has views as to what needs to be done, the approval of internal audit plans and budget is an audit committee responsibility. The varying views of the key parties must be jointly considered and appropriately reconciled, but the audit committee has the final word here.

As discussed in prior chapters, senior management and the board audit committee have traditionally been more concerned with financial accounting, SOx, and overall corporate governance rules than they have been with specific IT governance matters. These activities are defined through an annual internal audit plan prepared by internal audit and approved by the audit committee.

Audit committee reviews of all internal audit plans are essential if the policies and plans for the future are to be determined most effectively. The audit committee should assume this high-level coordination role, such that all interested parties (e.g., enterprise management, internal auditors, and external audit alike) can better understand the nature of the total internal audit plan and what to expect from the suppliers of audit services. Although there are practical limitations as to how actively the audit committee can become involved in the detailed planning process, some involvement has a demonstrated high value. Typically, the chair of the audit committee is the most active person in this plan review, but even this person is subject to time limitations. Internal audit should prepare a comprehensive set of annual planning documents for the committee that give detailed plans for the upcoming year, as well as longer-range plans for the future. In addition, internal audit should prepare summarized reports of past audit

activities and reassessments of its coverage to give the audit committee an understanding of significant areas covered in past reviews. Although internal audit should report its activities to the audit committee on a regular basis, this summary reporting of past activity gives an overview of their areas of audit emphasis as well as highlighting any potential gaps in audit coverage.

Internal audit plans with an IT governance perspective sometimes can present problems for enterprise audit committee members. These very senior people often are not aware of some of the IT-related governance issues discussed in these chapters, such as PCI DSS management, discussed in Chapter 11. The CAE, with support of the IT audit team, should take extra steps to educate the audit committee as to why it feels certain more technical IT issues are important from an internal controls and IT governance risk perspective.

AUDIT COMMITTEE BRIEFINGS AND IT GOVERNANCE ISSUES

For some senior-level managers serving on audit committees, IT governance issues and concerns may be unfamiliar, with sometimes strange-sounding issues. Audit committee–level executives often have become familiar with a limited number of IT-related governance issues, such as the importance of effective IT continuity plans, potential legal liabilities because of social network computing issues, or the risks of software viruses. Many business publications directed to audit committee–level executives have talked about types of risks and related IT governance issues. However, senior management, the CAE, and the enterprise IT audit function should try to communicate their concerns about more technical and related governance issues to their audit committee members.

IT governance audit review plans and risk concerns are part of overall internal audit plans, and IT auditors should have open access to their CAE regarding review of these specific IT governance issues. Getting messages to the audit committee, however, is sometimes a greater problem. As discussed, audit committee members are very involved with financial reporting issues, SOx compliance, and other risk issues, but many do not regularly focus on IT governance–related internal audit issues. Using the CAE as the prime contact, IT audit needs to reach out to audit committee members to brief them on important and evolving IT governance internal control issues.

For many enterprises, there may be value in scheduling a quarterly audit committee briefing on enterprise IT governance risks and evolving issues. These briefings could be used to educate audit committee members on the enterprise IT governance environment and any risk issues. This type of briefing sometimes can be done in conjunction with the enterprise's chief information officer, but often it is better for the session to be led primarily by the CAE and the enterprise's IT audit function.

An audit committee's most important responsibility is to review and take action on significant audit findings that are reported to them by internal and external auditors, management, and others. Although the audit committee has responsibility for all of these areas, our focus here is on the need for the audit committee internal audit, and IT audit in particular, to review and understand all significant IT governance findings and issues reported to them and to take appropriate action on a regular and prompt basis.

Reacting to significant audit findings that have been reported to the audit committee requires a combination of understanding, competence, and cooperation by all of the major interested parties—internal audit, management, external auditors, and the audit committee itself. Total enterprise welfare then becomes the standard by which to judge all internal audit services, as opposed to more provincial views where the interests of management and the audit committee may conflict to some extent. Within its own area of responsibility, IT management should act aggressively in exercising ongoing governance improvement actions to assess whether appropriate corrective action items are in place.

This and prior chapters have introduced and discussed a wide range of IT governance issues impacting a business enterprise. While the audit committee is responsible for ultimately assessing progress and activities regarding these matters, senior management responsible for enterprise IT governance should determine that adequate processes have been installed and that they are operating correctly. A good system of IT governance controls and processes will contribute to overall enterprise success.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

About the Author

ROBERT R. MOELLER, CPA, CISA, CISSP, AND PMP, is an internal audit, internal controls, and project management specialist with a strong understanding of corporate governance, information systems, and risk management. He has over 40 years of experience directing internal audit functions, managing a wide range of IT and other projects on governance and internal controls. He was the national director of IT auditing for Grant Thornton and was the internal audit director for Sears Roebuck, where he reported to the audit committee, led a team to reengineer the corporation's internal control processes, and launched their corporate ethics function. A frequently published author and speaker, he provides insights into many IT and business issues and concerns impacting enterprise governance, risk, and compliance processes.

Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Robert R. Moeller.
© 2013 John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc.

Index

Application portfolios, IT portfolio management, 260
Application systems development, 264
  enterprise resource planning (ERP) systems, 264
  ERP systems, 264
  rapid application development (RAD), 267
  systems development life-cycle (SDLC) processes, 264
AS5, risk-based approaches, 27
AS5 rules, Section 404 internal controls assessments, 17
Assignment of authority and responsibility, COSO control environment components, 56
Audit committee internal control issues, IT governance, 375
Audit committees
  IT governance responsibilities, 374
  SOx rules, 23, 372
Audit evidence classifications, internal audit processes, 328
Auditor Independence, Sarbanes-Oxley Act (SOx), 18
Availability management, ITIL service strategy processes, 96

Basic accounting cycles, Section 404 internal controls assessments, 15
Benchmarking, internal control evaluation processes, 62
Best practices standards for IT service support, 288
Board of directors and audit committee
  COSO control environment components, 55
  IT governance, 371
Business Continuity Plan (BCP) Life Cycle, IT governance, 190
Business continuity planning (BCP)
  BCP standards, 189
  disaster recovery planning, 188
  IT governance, 188
  IT security practices, 192
Business continuity planning (BCP) standards, 189
Business performance, IT Governance Concepts, 6

Capacity management, ITIL service strategy processes, 95
CEO financial report certification
  criminal penalties, 24
  officer disclosure sign-off, 24
  Sarbanes-Oxley Act (SOx), 23
Change management processes, IT governance, 100
Charging for IT services, ITIL financial management, 94
Client-server systems applications development, 268
Cloud computing application controls
  IT application controls, 164
  SAS 70, 164
Cloud computing concepts, 164
  IT governance and assurance issues, 165
  security and privacy challenges, 166
Cloud computing data location issues, IT governance concerns, 167
Cloud computing data segregation, IT governance concerns, 167
Cloud computing descriptions, IT concepts, 162
Cloud computing investigative support, IT governance concerns, 167
Cloud computing IT governance and assurance issues, cloud computing concepts, 165
Cloud computing long-term viability issues, IT governance concerns, 167
Cloud computing recovery issues, IT governance concerns, 167
Cloud computing regulatory compliance, IT governance concerns, 167
CMDB. *See* Configuration management database
COBIT
  COSO internal control framework, 71
  ISO 38500 principles, 119
  IT Governance Institute (ITGI), 68
  IT governance principles, 70
  IT-oriented internal control assessments, 67
  SOx internal controls requirements, 71, 84
  SOx Section 404, 84
  Val IT best practices governance framework, 298
COBIT governance objectives
  enterprise goals, 76
  governance definition, 81
COBIT financial governance objectives, enterprise goals, 77
COBIT 5 simplified general architecture, IT architecture enablers, 73
COBIT internal stakeholder needs, 74
COBIT IT security guidance, IT security model concepts, 185
COBIT principles
  IT architecture enablers, 72
  IT governance and management, 80
  IT governance value objectives, 75
  IT risk management enablers, 78
COBIT processes, management of enterprise IT, 81
COBIT strengths, IT governance focus, 85
COBIT enablers
  enabler concepts, 80
  types of, 79
Code of conduct stakeholder communications, enterprise codes of conduct, 344
Code violations and corrective actions, enterprise codes of conduct, 345
Codes of ethics, Senior Financial Officer SOx requirements, 26
Commitment to competence, COSO control environment components, 55
Communications and information, COSO internal control framework, 59
Compliance internal controls, COSO internal control framework, 53
Computers at risk (CAR), U.S. National Research Council, 179
Configuration management database (CMDB), processes, 102
Configuration management database (CMDB) components
  conceptual view, 256
  configuration items (CIs), 252

Configuration management database (CMDB) components (*continued*)
database configuration management facilities, 255
database federation, 257
data integration and management repositories, 255
data synchronization, 258
IT configuration management systems, 247
ITIL transition management processes, 101
security and data protection controls, 255
security and user access tools, 255
Configuration management definition, IT configuration management concepts, 249
Conflict-of-interest provisions, Sarbanes-Oxley Act (SOx), 26
Constant improvements program, GLBA Safeguards compliance, 206
Continuity management, ITIL service strategy processes, 98
Control activities
COSO Internal Control Framework, 57
functional or activity management, 58
information processing, 58
performance indicators, 58
physical controls, 58
segregation of duties, 58
top-level reviews, 58
Control environment, COSO internal control framework, 54
Corporate ethics, IT governance concepts, 9
Corporate responsibilities, Sarbanes-Oxley Act (SOx) , 22
COSO, COSO internal control framework, 53
COSO, National Commission on Fraudulent Financial Reporting, 52
COSO components and COBIT objectives, mapping IT governance relationships, 85
COSO control environment, tone at the top, 54
COSO control environment components
assignment of authority and responsibility, 56
board of directors and audit committee, 55
commitment to competence, 55
human resources policies and procedures, 56
integrity and ethical values, 55
management philosophy and operational style, 55
organizational structure, 56
COSO enterprise risk management (ERM) framework, IT governance concepts, 30
COSO ERM
control activities, 149
documentation, 148
enterprise risk management, 134
COSO ERM framework
control activities, 148
event identification, 141
information and communication, 149
internal environment, 138
risk responses, 145
monitoring, 151
objective setting, 140
risk appetite, 135
risk appetite map, 139
risk assessment, 144
risk management philosophy, 138
COSO ERM monitoring
framework, 151
process flowcharting, 152
risk monitoring activities, 151
COSO ERM risk event–risk response activities, 147
COSO internal control framework
COBIT, 71
communications and information, 59
compliance internal controls, 53
control activities, 57
control environment, 54
COSO, 53
definition, 49
dimensions of all internal controls, 64
financial reporting internal controls, 53
foundation components, 60
impact on IT governance, 54
importance of COSO internal controls, 66
internal controls definition, 53
internal control evaluation processes, 62
IT audit guidance, 68
IT governance guidance, 68
IT governance objectives, 49
IT-related internal controls, 50
monitoring, 60
monitoring guidance, 65
operations internal controls, 53
risk assessment, 57
standards background, 51
Treadway Commission, 52
COSO monitoring design and implementation process, internal control evaluation processes, 65
COSO risk assessment processes, internal control framework, 57
Costs and benefits, IT security, 180
Criminal penalties, CEO financial report certification, 24
Cryptography, HIPAA security requirements, 211

Database configuration management facilities, CMDB components, 255
Database federation, CMDB components, 257
Data management database repository, CMDB components, 255
Definition of internal control
internal control standards background, 51
SAS No. 1, 51
Definition of IT governance
IT governance concepts, 29
IT governance objectives, 30
Deming, Edward M., quality management standards, 112
Design-time policies, IT service-oriented architecture (SOA), 240
Design-time SOA processes, SDLC processes, 240
Dimensions of all internal controls, COSO internal control framework, 64
Disaster recovery planning
business continuity planning, 188
IT continuity planning, 187
Document archiving, ECM features, 313
Document classification processes, ECM features, 315
Document governance management, ECM features, 316

ECM architecture, IT governance, 313
ECM concepts, IT applications internal controls, 310
ECM features
document archiving, 313
document classification processes, 315
document governance management, 316
ECM processes, IT governance, 310
ECM security tools, IT security processes, 313
Effective risk management programs, GRC concepts, 40
Enabler concepts, COBIT types of enablers, 80
Enron failure, IT governance issues, 9
Enterprise business risks, risk management fundamentals, 129
Enterprise codes of conduct
code of conduct stakeholder communications, 344
code violations and corrective actions, 345
IT governance, 341
whistleblower and hotline functions, 346
Enterprise compliance challenges, GRC compliance, 42
Enterprise compliance issues, government rules and laws, 37
Enterprise compliance scope, GRC compliance, 44
Enterprise content management (ECM), IT governance, 309
Enterprise ethics, IT governance, 337
Enterprise ethics hotline functions, IT governance, 350

Enterprise goals
COBIT governance objectives, 76
COBIT financial governance objectives, 77
Enterprise governance, ethics programs, 352
Enterprise governance concepts, GRC Principles, 40
Enterprise governance issues, IT governance, 28
Enterprise IT governance goals, IT governance concepts, 7
Enterprise organization issues, IT governance concepts, 32
Enterprise resource planning (ERP) systems
application systems development, 264
ERP objectives and requirements, 271
ERP system configuration, 270
tangible and intangible ERP system benefits, 272
Enterprise risk management, COSO ERM, 134
Environmental risk analysis, GLBA safeguards compliance, 206
ERM components, information and communication flows, 150
ERP system configuration, 270
ERP systems, application systems development, 264
Ethical standards, SOx compliance processes, 27
Ethical workplace cultures, IT governance, 337
Ethics programs, enterprise governance, 352
External auditor, internal controls review requirements, Section 404 internal controls assessments, 19
External audit partner rotation, Sarbanes-Oxley Act (SOx), 21

Facebook, social media system examples, 358
Facebook, using, 359
Federal whistleblower rules, whistleblower and hotline functions, 348
Financial management for IT services, ITIL service strategy components, 93
Financial management of IT systems, IT governance, 95
Financial privacy rules, Gramm-Leach-Bliley Act (GLBA), 204
Financial reporting internal controls, COSO internal control framework, 53
Functional or activity management, control activities, 58

GASSP, implementing IT security principles, 183
GASSP body of knowledge, IT security standards, 184
GASSP principles, IT security purposes, 179
Generally accepted system security principles (GASSP), IT security standards, 179
GLBA, IT security standards, 203
GLBA Pretexting Rules, 206
GLBA Safeguards compliance
constant improvements program, 206
environmental risk analysis, 206
monitoring and auditing, 206
GLBA safeguards rule, Gramm-Leach-Bliley Act (GLBA), 205
Governance definition, COBIT governance objectives, 81
Governance, risk and compliance issues, GRC Principles, 38
Governance, risk, and compliance processes, IT governance, 45
Government rules and laws, enterprise compliance issues, 37
Gramm-Leach-Bliley Act (GLBA)
financial Privacy Rules, 204
GLBA Safeguards Rule, 205
IT governance rules, 205
IT privacy legislation, 203
IT security standards, 203
pretexting, 203
GRC capability model, OCEG Red Book, 292
GRC capability model elements, Open Compliance and Ethics Group (OCEG), 293
GRC compliance
enterprise compliance challenges, 42
enterprise compliance scope, 44
risk management overview, 42
GRC concepts, effective risk management programs, 40
GRC governance elements, IT governance concepts, 41
GRC guidance, Open Compliance and Ethics Group (OCEG), 292
GRC principles
enterprise governance concepts, 40
governance, risk, and compliance issues, 38
IT Governance Concepts, 39

Health Insurance Portability and Accountability Act (HIPAA), IT privacy rules, 208
HIPAA
IT governance requirements, 212
IT privacy rules, 208
IT security administrative procedures, 213
HIPAA patient record privacy rules
IT privacy rules, 209
medical records disclosures, 210
HIPAA security requirements
cryptography, 211
security services and mechanisms, 214
Human resources policies and procedures, COSO control environment components, 56

Impact of social media computing
IT governance, 365
IT system risks, 365
social media systems, 364
Impact on IT governance, COSO internal control framework, 54
Implementing IT configuration management, IT governance, 253
Implementing IT security principles
GASSP, 183
IT security standards, 183
Importance of COSO internal controls, COSO internal controls framework, 66
Incident management, ITIL service operation processes, 103
Information and communication flows, ERM components, 150
Information processing, control activities, 58
Information Systems Audit and Control Association (ISACA), IT auditors, 323
Information systems security, ITIL service strategy processes, 98
Information Technology Infrastructure Library (ITIL)
IT Service Management (ITSM), 87
ITIL continuous feedback cycle, 89
ITIL fundamentals, 88
Infrastructure portfolios, IT portfolio management, 260
Inherent risk, risk management fundamentals, 144
Institute of Internal Auditors (IIA)
Internal audit background, 321
internal audit standards, IT governance standards, 329
IT auditors, 323
Integrity and ethical values, COSO control environment components, 55
Internal audit background
Institute of Internal Auditors (IIA), 321
Internal audit responsibilities, 320
Internal audit charters, internal audit processes, 325
Internal audit processes
audit evidence classifications, 328
internal audit charters, 325
IT Governance Focus Areas, 330
performing internal audits, 327
planning and authorizing internal audits, 324
reporting internal audit results, 328
testing audit evidence, 327

Internal audit responsibilities
audit committees, 373
internal audit background, 320
Internal audit reviews
IT performance measurement processes, 333
IT resource management processes, 332
IT risk management processes, 332
IT value delivery processes, 331
Internal audit roles, Section 404 internal controls assessments, 15
Internal control deficiencies, internal control reporting processes, 62
Internal control definition, COSO internal controls, 49
Internal control evaluation processes
benchmarking, 62
COSO internal control framework, 62
COSO monitoring design and implementation process, 66
internal control monitoring processes, 65
Internal control issues, IT service-oriented architecture (SOA), 235
Internal control monitoring processes, internal control evaluation processes, 65
Internal control planning considerations, Section 404 internal controls assessments, 16
Internal control reporting processes
internal control deficiencies, 62
materiality considerations, 63
Internal control standards background
COSO internal controls, 51
definition of internal control, 51
Internal controls definition
COSO internal control framework, 53
IT internal controls, 50
Internal Organization for Standards, (ISO), 110
International Information Systems Security Certification Consortium $(ISC)^2$, IT security standards, 179
ISACA, IT Governance Institute (ITGI), 68
$(ISC)^2$, IT security standards, 179
ISO 27002, ISO IT security standards, 115
ISO 27002 implementation steps, IT security management processes, 117
ISO 27002 standards topic areas, ISO IT security standards, 116
ISO 38500 enterprise IT governance model, ISO standards, 121
ISO 38500 implementation steps, IT governance guidance, 122
ISO 38500 IT governance standards, ISO standards, 118
ISO 38500 objectives, IT governance, 120
ISO 38500 principles, COBIT, 119
ISO 9000 quality management standards
ISO standards, 112
quality management system process, 114
ISO certification process, ISO standards, 111
ISO Documentation hierarchy, ISO standards, 114
ISO IT security guidance, IT security model concepts, 185
ISO IT security standards
ISO 27002, 115
ISO 27002 Standards Topic Areas, 116
ISO standards
internal organization for standards, 110
ISO 38500 enterprise IT governance model, 121
ISO 38500 IT governance standards, 118
ISO 9000 quality management standards, 112
ISO certification process, 111
ISO documentation hierarchy, 114
quality management standards, 112
IT accounting, ITIL financial management, 94
IT application controls, cloud computing application controls, 164
IT application of management, IT portfolio management, 259
IT applications, internal controls
ECM concepts, 310
storage management virtualization, 168
IT applications, social media systems, 355
IT architecture enablers
COBIT 5 simplified general architecture, 73
COBIT principles, 72
IT architectures
IT service-oriented architecture (SOA), 232
service-driven IT applications, 232
IT audit guidance, COSO internal controls framework, 68
IT audit review activities, IT governance, 333
IT auditors
Information Systems Audit and Control Association (ISACA), 323
Institute of Internal Auditors (IIA), 323
IT budgeting, ITIL financial management, 93
IT capacity management, IT configuration management concepts, 250
IT cloud computing concepts, cloud computing descriptions, 162
IT configuration management, ITIL best practices, 251
IT configuration management concepts
configuration management definition, 249
IT capacity management, 250
IT governance issues, 250
IT problem management, 250
service level agreements (SLAs), 250
IT configuration management systems
configuration management database (CMDB), 247
IT governance, 247
IT infrastructure components, 248
ITIL best practices, 248
IT continuity planning
disaster recovery planning, 187
IT governance, 186
IT customer needs, IT service catalogs, 220
IT general controls, ITIL strategic capabilities, 92
IT governance
audit committee internal control issues, 375
board of directors and audit committee, 371
Business Continuity Plan (BCP) Life Cycle, 190
business continuity planning, 188
change management processes, 100
configuration management processes, 102
ECM Architecture, 313
ECM processes, 310
enterprise codes of conduct, 341
enterprise content management (ECM), 309
enterprise ethics hotline functions, 350
enterprise governance issues, 28
ethical workplace cultures, 337
financial management of IT systems, 95
governance, risk, and compliance processes, 45
impact of social media computing, 365
implementing IT configuration management, 253
internal audit processes, 324
ISO 38500 Objectives, 120
IT audit review activities, 333
IT configuration management systems, 247
IT continuity planning, 186
IT portfolio management, 259
IT service catalog business relationships, 222
IT service functions, 233
IT service level agreements (SLAs), 287
IT service-oriented architecture (SOA), 242
IT systems development processes, 264
IT systems security objectives, 99
IT value management initiatives, 300
IT virtualization, 170

ITIL service delivery best practices, 106
mission statements, 337
OCEG model, 297
Open Compliance and Ethics Group (OCEG), 153, 292
Payment Card Industry Data Security Standard (PCI DSS), 195
program management office (PMO), 284
project, program, and portfolio management overview, 286
RAD Controls and Procedures, 269
SLAs, 287
social media applications, 370
tangible and intangible ERP system benefits, 272
Val IT, 298
Val IT framework, 299
IT governance risk issues, IT governance concepts, 30
IT governance and management, COBIT principles, 80
IT governance cloud computing concerns
cloud computing data location issues, 167
cloud computing investigative support, 167
cloud computing long-term viability issues, 167
cloud computing recovery issues, 167
cloud computing regulatory compliance, 167
privileged user access issues, 167
IT governance concepts
business performance, 6
corporate ethics, 9
COSO enterprise risk management (ERM) framework, 30
definition of IT governance, 29
enterprise IT governance goals, 7
enterprise organization issues, 32
GRC governance elements, 41
GRC principles, 38
IT governance risk issues, 30, 31
IT governance enterprise issues, 33
IT governance security issues, 34
IT security controls, 34
jurisdiction and boundary issues, 32
legislative and regulatory issues, 32
measures of IT governance success, 6
risk appetite, 31
risk management concerns, 40
Sarbanes-Oxley Act (SOx) rules, 5
IT governance controls, IT service-oriented architecture (SOA), 245
IT governance elements
GRC concepts, 39
Sarbanes-Oxley Act (SOx), 10
IT governance enterprise issues, IT governance concepts, 33
IT governance focus, COBIT strengths, 85
IT governance focus areas, internal audit processes, 330
IT governance guidance
COSO internal controls framework, 68
ISO 38500 implementation steps, 122
IT Governance Institute, Val IT, 298
IT Governance Institute (ITGI)
COBIT, 68
ISACA, 68
IT governance issues
Enron failure, 9
IT configuration management concepts, 250
IT service-oriented architecture (SOA), 235
risk management fundamentals, 126
security issues, 34
smartphone and handheld devices, 175
SOA implementation blueprint, 241
SOA policies and procedures, 238
IT governance objectives
COSO internal controls, 49
definition of IT governance, 30
OCEG GRC capability model, 154
IT governance policies, smartphone and handheld devices, 176
IT governance principles, COBIT, 70
IT governance requirements, HIPAA, 212
IT governance responsibilities, audit committees, 374
IT governance risk issues
IT governance concepts, 31
IT password standards, 31
risk appetite, 31
IT governance risks, social media systems, 355
IT governance rules, Gramm-Leach-Bliley Act (GLBA), 205
IT governance security issues, IT governance concepts, 34
IT governance standards, Institute of Internal Auditors (IIA) internal audit standards, 329
IT governance value objectives, COBIT principles, 75
IT governance virtualization good practices, 174
IT infrastructure
service delivery best practices, 88
service support processes, 89
IT infrastructure components, IT configuration management systems, 248
IT internal controls, definition, 50
IT management concerns, IT security, 178
IT objectives, IT-related COBIT goals, 83
IT operations, IT service level agreements (SLAs), 291
IT password standards, IT governance risk issues, 31
IT performance measurement processes, internal audit reviews, 333
IT portfolio management
application portfolios, 260
infrastructure portfolios, 260
IT application of management, 259
IT governance, 259
project portfolios, 261
project, program, and portfolio management overview, 283
IT privacy legislation, Gramm-Leach-Bliley Act (GLBA), 203
IT privacy rules
Health Insurance Portability and Accountability Act (HIPAA), 208
HIPAA patient record privacy rules, 209
IT problem management, IT configuration management concepts, 250
IT program management
project, program, and portfolio management overview, 283
IT project management
project, program, and portfolio management overview, 283
IT resource management processes, internal audit reviews, 332
IT risk management enablers, COBIT principles, 78
IT risk management processes, internal audit reviews, 332
IT security
costs and benefits, 180
IT management concerns, 178
management practices, 180
societal factors constraints, 182
systems owners security responsibilities, 181
IT security administrative procedures, HIPAA, 213
IT security controls, IT governance concepts, 34
IT security management processes, ISO 27002 implementation steps, 117
IT security model concepts
COBIT IT security guidance, 185
ISO IT security guidance, 185
IT security practices, business continuity planning, 192
IT security processes, ECM security tools, 313
IT security purposes, GASSP principles, 179
IT security standards
$(ISC)^2$, 179
GASSP body of knowledge, 184
generally accepted system security principles (GASSP), 179
GLBA, 203
Gramm-Leach-Bliley Act (GLBA), 203
implementing IT security principles, 183
International Information Systems Security Certification Consortium $(ISC)^2$, 179
Payment Card Industry Data Security Standard (PCI DSS), 195
IT service catalog business relationships, IT governance, 222

IT service catalogs
IT customer needs, 220
IT system of record, 221
service catalog characteristics, 218
service request processes, 220
IT service functions, IT governance, 233
IT service level agreement (SLA) contents, 290
IT service level agreements (SLAs)
IT governance, 287
IT operations, 291
IT service level agreement contents, 290
IT Service Management Forum (itSMF), 287
Information Technology Infrastructure Library (ITIL), 87
IT Service Management Forum (itSMF)
best practices standards for IT service support, 288
IT service level agreements (SLAs), 287
ITIL, 288
IT service-oriented architecture (SOA)
design-time policies, 240
internal control issues, 235
IT architectures, 232
IT governance controls, 245
IT governance issues, 235
SOA characteristics, 232
web services applications, 243
IT system of record, IT service catalogs, 221
IT system risks, impact of social media computing, 365
IT systems development efforts, project management, 275
IT systems development processes, IT governance, 264
IT systems internal controls, IT virtualization, 173
IT systems security objectives, IT governance, 99
IT systems virtualization, definition, 162
IT value delivery processes, internal audit reviews, 331
IT value management initiatives, IT governance, 300
IT value management readiness assessment, Val IT, 301
IT virtualization
IT governance, 170
IT governance virtualization good practices, 174
IT systems internal controls, 173
virtualization definitions, 169
ITIL
IT Service Management Forum (itSMF), 288
service delivery best practices, 88
service feedback processes, 90
service support processes, 89
ITIL best practices, IT configuration management, 251
ITIL change management, ITIL service strategy processes, 100
ITIL continuous feedback cycle, Information Technology Infrastructure Library (ITIL), 89
ITIL financial management
charging for IT services, 94
IT accounting, 94
IT budgeting, 93
ITIL service strategy components, 93
ITIL fundamentals
Information Technology Infrastructure Library (ITIL), 88
ITIL service operation processes, 103
service strategy components, 91
ITIL incident management life cycle, service operation event and incident management, 104
ITIL service delivery best practices, IT governance, 106
ITIL service operation processes
incident management, 103
ITIL fundamentals, 103
problem management, 105
service operation event and incident management, 103
service operation problem management, 105
ITIL service strategy components
financial management for IT services, 93
ITIL financial management, 93
ITIL service strategy processes
availability management, 96
capacity management, 95
continuity management, 98
information systems security, 98
ITIL change management, 100
service delivery availability management, 96
service delivery capacity management, 95
service delivery continuity management, 98
service delivery information systems security, 98
service transition change management, 100
ITIL strategic capabilities, IT general controls, 92
ITIL transition management processes
configuration management, 101
service transition configuration management, 101
IT-oriented internal control assessments, COBIT, 67
IT-related COBIT goals
IT objectives, 83
mapping COBIT processes, 82
IT-related internal controls, COSO internal controls, 50

Johnson & Johnson Tylenol crisis, mission statements, 338
Jurisdiction and boundary issues, IT governance concepts, 32

Legislative and regulatory issues, IT governance concepts, 32
LinkedIn
market research application, 360
social media system examples, 360

Management of enterprise IT, COBIT processes, 81
Management philosophy and operational style, COSO control environment components, 55
Management practices, IT security, 180
Mapping COBIT processes, IT-related COBIT goals, 82
Mapping IT governance relationships, COSO Components and COBIT Objectives, 85
Market research application, LinkedIn, 360
Materiality considerations, internal control reporting processes, 63
Measures of IT governance success, IT governance concepts, 6
Medical records disclosures, HIPAA patient record privacy rules, 210
Mission statements
IT governance, 337
Johnson & Johnson Tylenol crisis, 338
Mitigation strategies, risk identification, 41
Monitoring, COSO Internal Control Framework, 60
Monitoring and auditing, GLBA safeguards compliance, 206
Monitoring guidance, COSO internal control framework, 65

National Commission on Fraudulent Financial Reporting
COSO, 52
Treadway Commission, 52

OCEG GRC capability model
GRC subpractices, 159
IT governance objectives, 154
Principled Performance, 154
OCEG model, IT governance, 297
OCEG Red Book
GRC capability model, 292
Open Compliance and Ethics Group (OCEG), 153
Officer disclosure sign-off, CEO financial report certification, 24
Open Compliance and Ethics Group (OCEG)
GRC capability model elements, 293
GRC guidance, 292
IT governance, 153, 292
OCEG Red Book, 153
Principled Performance concept, 292
risk management, 153
Operations internal controls, COSO internal control framework, 53
Organizational structure, COSO control environment components, 56

Payment Card Industry (PCI) Data Security Standards Council, 196
Payment Card Industry Data Security Standard (PCI DSS)
  IT governance, 195
  IT security standards, 195
  Payment Card Industry (PCI) Council, 196
  self-assessment processes, 202
Payment card requirements, PCI DSS, 197
PCAOB (Public Company Accounting Oversight Board), Sarbanes-Oxley Act (SOx), 10
PCI DSS (Payment Card Industry Data Security Standard)
  IT governance, 195
  IT security standards, 195
  Payment Card Industry (PCI) Council, 196
  self-assessment processes, 202
Performance indicators, control Activities, 58
Performing internal audits, internal audit processes, 327
Physical controls, control activities, 58
Planning and authorizing internal audits, internal audit processes, 324
PMBOK. *See* Project Management Book of Knowledge (PMBOK)
Pretexting
  GLBA pretexting rules, 206
  Gramm-Leach-Bliley Act (GLBA), 203
PRINCE2, project management standards, 280
PRINCE2 project management process, project management standards, 282
Principled Performance, OCEG GRC capability model, 154
Principled Performance concept, Open Compliance and Ethics Group (OCEG), 292
Privileged user access issues, IT governance cloud computing concerns, 167
Pro forma financial reports, Sarbanes-Oxley Act (SOx), 25
Problem management
  ITIL service operation processes, 105
  request for change (RFC) documents, 105
Process flowcharting, COSO ERM monitoring, 152
Program management office (PMO), IT governance, 284
Project definition, *Project Management Book of Knowledge* (PMBOK), 277
Project management, IT systems development efforts, 275
Project Management Book of Knowledge (PMBOK)
  process groups and knowledge areas, 279
  project definition, 277
  Project Management Institute (PMI), 276
  project management process, 278
  project management standards, 276
Project Management Institute (PMI), *Project Management Book of Knowledge* (PMBOK), 276
Project management standards
  PRINCE2, 280
  PRINCE2 Project Management Process, 282
  Project Management Book of Knowledge (PMBOK), 276
Project portfolios, IT portfolio management, 261
Project, program, and portfolio management overview
  IT governance, 286
  IT portfolio management, 283
Public Company Accounting Oversight Board (PCAOB), Sarbanes-Oxley Act (SOx), 10

Qualitative risk assessments, risk management fundamentals, 128
Quality management standards
  ISO standards,
  Deming, Edward, 112
Quality management system process, ISO 9000 quality management standards, 114
Quantitative risk assessments, risk management fundamentals, 128

RAD controls and procedures, IT governance, 269
Rapid application development (RAD)
  application systems development, 267
  client–server systems applications development, 268
Reporting internal audit results, internal audit processes, 328
Request for change (RFC) documents, problem management, 105
Requirements analysis process, systems development life-cycle (SDLC) phases, 266
Residual risk, risk management fundamentals, 144
Risk acceptance, risk management strategies, 146
Risk appetite
  COSO ERM framework, 135
  IT governance concepts, 31
  IT governance risk issues, 31
Risk appetite map, COSO ERM framework, 139
Risk assessment, COSO internal control framework, 57
Risk assessment analysis
  risk likelihood, 129
  risk significance, 129
Risk avoidance, risk management strategies, 145
Risk event–risk response activities, COSO ERM risk event–risk response activities, 147
Risk identification
  mitigation strategies, 41
  risk management fundamentals, 127
Risk impact, risk management fundamentals, 145
Risk likelihood
  risk assessment analysis, 129
  risk management fundamentals, 145
Risk Management, Open Compliance and Ethics Group (OCEG), 153
Risk management concerns
  IT governance concepts, 40
  risk monitoring, 42
Risk management fundamentals
  enterprise business risks, 129
  inherent risk, 144
  IT governance issues, 126
  qualitative risk assessments, 128
  quantitative risk assessments, 128
  residual risk, 144
  risk identification, 127
  risk impact, 145
  risk likelihood, 145
  risk monitoring, 133
  risk portfolio management, 147
  risk response planning, 131
Risk management overview, GRC compliance, 42
Risk management philosophy, COSO ERM framework, 138
Risk management strategies
  risk acceptance, 146
  risk avoidance, 145
  risk reduction, 145
Risk monitoring
  risk management concerns, 42
  risk management fundamentals, 133
Risk monitoring activities, COSO ERM monitoring, 151
Risk portfolio management, risk management fundamentals, 147
Risk reduction, risk management strategies, 145
Risk response planning, risk management fundamentals, 131
Risk significance, risk assessment analysis, 129
Risk-based approaches, AS5, 27
Runtime policies and processes, SOA governance, 241

Sarbanes-Oxley Act (SOx)
  audit committee financial expert rules, 23
  auditor independence, 18
  CEO financial report certification, 23
  conflict-of-interest provisions, 26
  corporate responsibilities, 22
  external audit partner rotation, 21
  external audit process rules, 12
  IT governance elements, 10
  pro forma financial reports, 25
  Public Company Accounting Oversight Board (PCAOB), 10

Sarbanes-Oxley (*continued*)
Section 404 internal controls assessments, 14
SOx key provisions summary, 11
SOx officer disclosure sign-off, 25
whistleblower rules, 23
Sarbanes-Oxley Act (SOx) rules, IT governance concepts, 5
SAS No. 1, definition of internal control, 51
SAS 70, cloud computing application controls, 164
SDLC life cycle, systems development life-cycle (SDLC) phases, 265
SDLC processes
design-time SOA processes, 240
SOA life cycle, 240
Section 404 internal controls assessments
AS5 rules, 17
basic accounting cycles, 15
external auditor service limitations, 19
internal audit roles, 15
internal control planning considerations, 16
Sarbanes-Oxley Act (SOx), 14
Security and data protection controls, CMDB components, 255
Security and privacy challenges, cloud computing concepts, 166
Security issues, IT governance issues, 34
Security services and mechanisms, HIPAA security requirements, 214
Segregation of duties, control activities, 58
Self-assessment processes, payment card industry data security standard, 202
Senior financial officer SOx requirements, codes of ethics, 26
Service catalog
characteristics, 223
elements, 223
IT service catalogs, 218
management, 224
Service delivery availability management, ITIL service strategy processes, 96
Service delivery best practices
IT infrastructure, 88
ITIL, 88
Service delivery capacity management, ITIL service strategy processes, 95
Service delivery continuity management, ITIL service strategy processes, 98
Service delivery information systems security, ITIL service strategy processes, 98
Service-driven IT applications, IT architectures, 232
Service feedback processes, ITIL, 90
Service level agreements (SLAs), SOA governance, 241
Service level agreements (SLAs), IT configuration management concepts, 250
Service operation event and incident management
ITIL incident management life cycle, 104
ITIL service operation processes, 103
Service operation problem management, ITIL service operation processes, 105
Service-oriented architecture. *See* SOA characteristics
Service request processes, IT service catalogs, 220
Service strategy components, ITIL fundamentals, 91
Service support processes
IT infrastructure, 89
ITIL, 89
Service transition change management, ITIL service strategy processes, 100
Service transition configuration management, ITIL transition management processes, 101
SLAs, IT governance, 287
Smartphone and handheld devices
IT governance issues, 175
IT governance policies, 176
SOA characteristics
enterprise IT general controls, 233
IT service-oriented architecture (SOA), 232
SOA enterprise configurations, 234
SOA service aggregation, 233
SOA enterprise configurations, SOA characteristics, 234
SOA governance
runtime policies and processes, 241
service level agreements, 241
stakeholder SOA life-cycle roles and responsibilities, 239
SOA implementation blueprint, IT governance issues, 241
SOA life cycle, SDLC processes, 240
SOA policies and procedures, IT governance issues, 238
SOA service aggregation, SOA characteristics, 233
Social media applications, IT governance, 370
Social media IT applications history, social media systems, 356
Social media policy, social media systems, 368
Social media system examples
Facebook, 358
LinkedIn, 360
Twitter, 362
Social media systems
impact of social media computing, 364
IT applications, 355
IT governance risks, 355
social media IT applications history, 356
social media policy, 368
Societal factors constraints, IT security, 182
SOx compliance processes, ethical standards, 27
SOx internal controls requirements, COBIT, 71, 84
SOx key provisions summary, Sarbanes-Oxley Act (SOx), 11
SOx officer disclosure sign-off, Sarbanes-Oxley Act (SOx), 25
SOx rules, audit committees, 372
SOx Section 404, COBIT, 84
Stakeholder SOA life-cycle roles and responsibilities, SOA governance, 239
Storage management virtualization, IT applications internal controls, 168
Systems development life-cycle (SDLC) phases
requirements analysis process, 266
SDLC life cycle, 265
Systems development life-cycle (SDLC) processes, application systems development, 264
Systems owners security responsibilities, IT security, 181

Tangible and intangible ERP system benefits
enterprise resource planning (ERP) systems, 272
IT governance, 272
Testing audit evidence, internal audit processes, 327
Tone at the top, COSO control environment, 54
Top-level reviews, control activities, 58
Treadway Commission
COSO internal controls framework, 52
National Commission on Fraudulent Financial Reporting, 52
Twitter, terms and concepts, 363

U.S. National Research Council, Computers at Risk (CAR), 179

Val IT
IT governance, 298
IT Governance Institute, 298
IT value management readiness assessment, 301
Val IT best practices governance framework, COBIT, 298
Val IT framework, IT governance, 299
Virtualization definitions, 162, 169

Web services applications, IT service-oriented architecture (SOA), 243
Whistleblower and hotline functions
enterprise codes of conduct, 346
Federal whistleblower rules, 348
Whistleblower rules, Sarbanes-Oxley Act (SOx), 23